Wireless Local Area Network (WLAN) Best Practices Guide

we envision

Government
of Alberta

Wireless Local Area Network (WLAN) Best Practices Guide

Alberta. Alberta Education. School Technology branch.
Wireless local area network (WLAN) best practices guide.

ISBN 978-0-7785-9694-3 (Print)
ISBN 978-0-7785-9695-0 (PDF)

Available online at: http://education.alberta.ca/admin/technology/research.aspx

1. Wireless LANs -- Handbooks, manuals, etc. 2. Wireless LANs – Security measures – Handbooks, manuals, etc. 3. Computer networks -- Handbooks, manuals, etc. I. Title.

TK5105.78 A333 2011 004.68

Table of Contents

Chapter 1 Introduction 4

Chapter 2 Wireless Technology Overview 6
- 2.1 Overview of Wireless Technology 6
- 2.2 Wireless Security Standards 17
- 2.3 Overview of Wireless Market and Vendors 24

Chapter 3 Going Wireless Preparation and Planning 28
- 3.1 First Steps 28
- 3.2 Analysis 29
- 3.3 Project Plan 39
- 3.4 Technical Deployment Considerations 43

Chapter 4 Security 59
- 4.1 Security Policy 59
- 4.2 Network Security 60
- 4.3 Wireless Security 64
- 4.4 Mobile Host Security 69
- 4.5 Content Security 71

Chapter 5 Innovation and Issues 72
- 5.1 Wireless Gigabit Alliance (Wi-Gig) 72
- 5.2 White-Fi 72
- 5.3 Real Time Location Services (RTLS) 72
- 5.4 Health & Safety Concerns 72

Appendix A Case Studies 74
- Calgary Board of Education 75
- Calgary Catholic School District 77
- Edmonton Public School District 79
- Wolf Creek School District 81
- Grande Prairie Public School District 83

Appendix B Implementation Resources 85

Appendix C Glossary of Terms and Acronyms 89

Appendix D Vendors 91

Chapter 1 Introduction

Alberta's Education System and Wireless Local Area Network (WLANs)

Four years ago, the original Wireless Local Area Network (WLAN) Best Practices Guide was released as WLANs began to be installed in Kindergarten to Grade 12 schools in Alberta. At that time, Alberta Education was launching the Emerge One-to-One Laptop Learning Initiative, and needed to provide technical advice to participating school authorities on best practices for implementing wireless networks. This advice was shared in the format of a best practices guide to allow all school authorities access the information.

Today, the wireless landscape continues to change. A growing number of devices rely on access to wireless networks to access information and run applications. The average user of these mobile devices now expects to have access to information at their fingertips, which is enabled by growing access to free wireless networks. The user who at one time had to pay to use Wi-Fi at airports, coffee shops and other public places now gets it for free with their coffee, groceries or boarding pass.

Within schools, the combination of wireless technology's relatively low cost and easy deployment has led many districts implementing wireless technology without adequate up front planning and without addressing ongoing support requirements. This has often led to degraded levels of service and significant security exposures, dramatically increasing failure rates of user adoption and hindering seamless usage.

To adequately protect information security and provide reliable service, school districts contemplating WLANs must address their network security and ongoing management practices, including associated tools. The ability to deliver information and resources for education using WLAN technology will be improved by delivering consistent and reliable service.

Audience

The primary audience for this guide is IT directors and network personnel who are responsible for deploying and managing wireless related infrastructure in Alberta schools and supporting laptops and mobile devices in the classroom. All levels of IT staff at both the district and local school level can benefit from information included in this guide.This guide is not meant for educational coordinators or teachers.

Whether your district has already deployed some or even all of your schools with WLAN technology, or if you are just getting started, this guide will provide insight to all aspects of using wireless at your schools.

Sources

This guide was updated by SAIT Polytechnic in conjunction with Alberta Education.

Many resources have been included from an array of global leading manufacturers of wireless hardware, software and related technology solutions. Refer to the section marked Resources and Sources for a detailed list of helpful reference materials and websites. Several of the case studies in the original guide were revisited to see what has changed in the scope, hardware and implementation strategies being adopted by the school districts.

Scope

This guide is focused on WLANs and associated wireless technology. When addressing key aspects of technology such as WLANs, a comprehensive and holistic approach is required in order to truly derive an overall understanding of the complex, integrated and inter-dependent aspects of IT. Hence, further to wireless technology, the guide also delves into security issues. This area should be further addressed in order to gain a comprehensive understanding and view of wireless technology's role within your district's overall IT strategy.

How to Read and Use this Document

This document was created as a technical guide to assist K-12 school authorities in implementing WLANs. The guide may be read front-to-back or used as a reference for all aspects of the selection, configuration, security and ongoing management of WLANs.

This guide will walk you through the standards and protocols associated with wireless technology, the current market and some vendors, security strategies specific to wireless networks and to networks in general. Implementing solutions into your schools and information key to the ongoing management of your technology will also be addressed

For easy reference each chapter contains tips and recommendations listed in text boxes like the one below within their associated section.

Tips will be included throughout various sections of the Guide and appear in a graphic text box like this one on the corresponding page.

Chapter 2 Wireless Technology Overview

Wireless LANs are everywhere – in offices, homes, hotels, coffee shops and at the airport. The wireless concept that we take for granted now has its roots in the wireless modem of the early 90's. Early wireless modems were designed for single peripheral devices that needed a way to send and receive computer data. The modem speeds were more than adequate for the task.

One of the best things about WLANs is that they operate in a license-free band, allowing the market to develop products and technologies through open competition. Operating in unlicensed bands can also be a drawback, as it results in increasing radio interference from other devices such as cordless phones. Industry Canada determines the frequency bands that WLANs operate in and the Institute of Electrical and Electronics Engineers (IEEE) develops the standards that describe how the technology will work in that spectrum.

Industry professionals drawn to this field are typically from the Information Systems Networking field with a strong background in the concepts of wired LAN, MAN and WAN or from the radio telecommunications field with an in-depth experience in wireless communication. The WLAN field requires some degree of expertise in both. The hardware is typically added to an existing system as an extension of the access layer requirements of the network and managing the air interface requires another skill set entirely.

2.1 Overview of Wireless Technology

LANs, WLANs and Protocols

What Is Wi-Fi?

Wi-Fi stands for wireless fidelity. Personal computers (PCs) can be equipped with Wi-Fi adapters (which are available as internally-mounted cards, most typically a USB adaptor. Most laptops are standard now with a Wi-Fi interface that will handle all current Wi-Fi standards, including 802.11a/b/g/n. Wi-Fi adapters are fairly inexpensive. The adapters seek out signals broadcast by devices called access points (APs) that in turn are typically connected to the existing wired network. This gives Wi-Fi devices access to the same resources that devices connected to the wired network have. Although it is less common, Wi-Fi devices can also communicate directly (one-to-one) with each other. Wi-Fi devices, if capable, will adapt to the standard in use by APs within range and employ several different technical standards grouped together and referred to as the IEEE 802.11 specification in order to communicate with an AP.

What is the IEEE?

The Institute of Electrical and Electronics Engineers (IEEE) creates and finalizes standards for computer networks, amongst other technologies. The IEEE 802.11 specification defines how wireless networks communicate. As a comparison, most wired networks based on Ethernet and CSMA/CD (defined later) technology conform to the 802.3 standard.

The Wi-Fi Alliance, to which all enterprise product manufacturers belong, guides the development of standards through product testing.

For more information, visit www.ieee.org and www.wi-fi.org.

Standards for Communication: The 802.11 Specification

802.11

In 1997, the IEEE published the original 802.11 – 1997 standard. In the industry, it is often referred to as 802.11 prime as it was the initial wireless standard. It was revised in 1999 and reaffirmed in 2003 as 802.11 – 1999 (R2003). By this release, most of the following subsets of the standard have their own section devoted to the idiosyncrasies of each. The most recent standard, 802.11n - 2009 includes the much promised increase in data rates from 54Mb/s to 600 Mb/s. The original standard allowed for data rates at 1 or 2 Mb/s. It contained three clauses defining physical layers. In Clause 16 it defined an infrared physical layer which in the 802.11 form is obsolete. Clause 14 defined a Frequency Hopping Spread Spectrum (FHSS) physical layer. This technology has its roots as far back as WWII with the first known patent of its type. Clause 15 devices are defined as Direct Sequence Spread Spectrum (DSSS) and are the root of the subsequent amendments of 802.11a/b/g radio devices. The Clause 16 or infrared devices are not considered a radio frequency technology, and will not be considered in this document due to their obsolete nature.

All of the clause 14 and 15 devices or FHSS and DSSS devices operate in the 2.4 GHz Industrial, Scientific and Medical (ISM) Band as defined by Industry Canada. In Canada the IEEE restricts the operation of these devices to the Spectrum between 2.40 GHz and 2.4835 GHz. Clause 14 or FHSS devices are further restricted to 1 MHz wide carriers in the space between 2.402 GHz and 2.480 GHz, allowing a range of 78 individual carriers that can be organized into a pattern for the connected transmitter and receiver to follow in order to communicate. These FHSS radio devices cannot communicate with DSSS radio devices. As manufacturers decided where to spend their research and development capital, DSSS radio devices and their apparent capabilities caused many of the major vendors to focus on the future and development of Clause 15 devices. The amendments of 802.11b and g are evidence of this as both are backward compatible with Clause 15 DSSS 802.11 prime devices but cannot communicate with 802.11 Clause 14 FHSS devices. The most recent release of this standard introduced Clause 20, which defines the high throughput operation of the 2.4 .GHz and 5.8 GHz devices that comply with the 802.11n standard.

802.11b

In 1999, 802.11b – 1999 was released and was later amended into the 802.11 standard. It defines operation in the 2.4 GHz radio band and DSSS only. The capabilities of adding two additional data rates of 5.5 Mb/s and 11.0 Mb/s created an even greater separation of demand for what was available at that time. This gave DSSS a clear advantage over the legacy FHSS devices with their 2.0 Mb/s maximum data rate. These new data rates were defined as High Rate DSSS (HR-DSSS).

802.11a

A second IEEE task group finished its project during 1999, which was ratified as 802.11a – 1999. Its mandate had been to define technologies that could operate in the newly available Unlicensed National Information Infrastructure (UNII) band. This use of Spread Spectrum was called Orthogonal Frequency Division Multiplexing (OFDM). This was initially defined as 3 - 100 MHz wide bands in the 5.8 GHz range. They are more commonly known as **UNII-Low** 5.150 – 5.250 GHz, **UNII-Mid** 5.250 – 5.350 GHZ, and **UNII-Upper** 5.725 – 5.825 GHz. The lack of spectrum in the 2.4 GHz band required some additional spectrum allocation for wireless networks. More recently, a fourth band in the 5.8 GHz range was released and is known as the **UNII-New** 5.47 – 5.725 GHz band. 802.11a devices are classed as Clause 17 devices in the 802.11 – 1999 (R2003) version of the standard. These 802.11a devices are not compatible with any of the other 802.11 technologies as they operate in a separate portion of the radio spectrum. At the time of release, their data rates of 6/9/12/18/24/36/48 and 54 Mb/s were also incompatible with the 802.11 prime and 802.11b data rates. There are many multi-band cards available today that can support all 802.11a/b/g technologies.

802.11b/g

One amendment that was highly anticipated was the 802.11g – 2003 Std. These devices, defined as Clause 18 devices, operate in the 2.4 GHz spectrum, are compatible with the 802.11b legacy devices and capable of additional bandwidth. This standard combined the OFDM process of 6/9/12/18/24/36/48 and 54 Mb/s data rates in addition to the backward compatibility to the data rates of 802.11b. It is described as Extended Rate Physical OFDM (ERP-OFDM). Device with this capability can typically be configured as one of the following: 802.11b only, 802.11g only or 802.11bg. This will have an impact on the effective throughput of the infrastructure device. With the implementation of 802.11n standard devices, the 802.11b devices should be completely disabled and any should be upgraded to a higher speed network.

802.11g

When an 802.11b/g device is operating in the 802.11g mode, it operates as defined by Clause 19 of the standard and operates in the Orthogonal Frequency Division Multiplexing (OFDM) mode. This may also referred to as a pure "G" system. In this mode of operation, it will not communicate with or allow 802.11b clients to participate on the network. In systems that are migrating from a completely 802.11b network, this would be the eventual goal.

802.11n

With the 802.11n – 2009 ratification, major vendors have now included these products in the family of wireless adaptors and APs. The biggest visible difference with these devices is the addition of antennas to the AP. The standard uses additional spatial streams to allow for higher throughputs. The n standard also doubles the bandwidth of an 802.11 channel from 20 MHz to 40 MHz. These can be deployed in both the 2.4 GHz band as well as the 5.8GHz radio band. This standard is more suited to the 5.8 GHz range as there is sufficient bandwidth to allow for adjacent non-interfering APs whereas at 2.4 GHz, the bandwidth is limited to 84.5 MHz which allows only two adjacent non-interfering channels. When an 802.11n device is operating in this mode, its operation is defined by clause 20 of the standard and operates in the OFDM mode. This mode of operation, when there are no devices of previous standards that require backward compatibility, is often referred to as HT- greenfield format HT (High Throughput). The standard defines up to four concurrent streams of data which would have an aggregate throughput of 600 Mb/s. None of the currently released devices have all the "Radio Chains" present so the maximum throughput of the standard is still a few hardware releases away from reality. 802.11n has not provided any additional channels for use, only an aggregation of channels in a single AP or client to achieve higher throughput. With 802.11n, an AP can use up to 60 different rates from 6.5 Mb/s up to 300 Mb/s with the combinations of Modulation and Coding Scheme (MCS).

802.11i

The IEEE 802.11i standard focuses on addressing all aspects of wireless security—even beyond client authentication and data privacy using WEP keys. As the 802.11i standard was being developed, wireless LAN vendors have moved ahead to implement as many of its features as possible. As a result, the Wi-Fi Alliance developed *Wi-Fi Protected Access (WPA)* based on some of the 802.11 draft components.

This is the most recent version of encryption for wireless networks. It is defined as MAC Layer Security Enhancements for 802.11. It increases the encryption sophistication of WEP using the Advanced Encryption Standard (AES). The hardware of devices that use 802.11i must be designed to handle AES. The two are not compatible, they are completely unique. Older legacy 802.11 products are not upgradeable. For some administrators, this provides some issues if they are upgrading their entire system to an 802.11i based encryption. Some equipment may need to be replaced in order to comply.

Table 1 – 802.11 Speed Comparison

IEEE Wireless Specification Designation	Release Date	Operating Frequency Range	Throughput Speeds (maximum)	Effective Throughput Speeds (typical)	Range (typical indoor distance in meters)
802.11a	1999	5.15-5.35/5.47-5.725/5.725-5.875 GHz	54 Mb/s	22 Mb/s	~25 meters
802.11b	1999	2.4-2.5 GHz	11 Mb/s	5 Mb/s	~35 meters
802.11g	2003	2.4-2.5 GHz	54 Mb/s	22 Mb/s	~25 meters
802.11n	2009	2.4 GHz or 5 GHz bands	600 Mb/s	100 Mb/s	~50 meters

*Note that speed and ranges can vary dramatically based on environmental factors.

The effective throughput is limited by the half-duplex nature of this wireless technology, as well as the Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA described below) mechanism which governs the use of the channel. This throughput could be achieved by a single client device using a particular network access point by itself. The available bandwidth must be shared between all clients connected to a particular network access point.

The typical 802.11g device is also capable of 802.11b data rates, making the advertised range of all devices in the 2.4 GHz range the same. It is important to note that the advertised range is at the lowest data rate. 802.11a for example has 75 meters of range at 6 Mb/s.

How WLANs Communicate

As a client brings up its wireless connection, it must find an access point (AP) that is reachable and that will approve its membership. The client must negotiate its membership and security measures in the following sequence:

1. Use an SSID that matches the AP.
2. Authenticate with the AP.
3. Use a packet encryption method (data privacy) *(optional)*.
4. Use a packet authentication method (data integrity) *(optional)*.
5. Build an association with the AP.

The following sections outline wireless communication, followed by an overview of wireless security. Chapter 4 is dedicated to a more robust explanation of wireless security, and includes network security. As well, this chapter highlights other interrelated elements of security which may not be directly relevant to WLANs, however are integral to understanding and properly managing WLAN in K-12 school authorities.

Wireless Signals

There are three spread spectrum wireless technologies and they are not interoperable. The three technologies are direct sequence spread spectrum, frequency hopping spread spectrum and infrared. The OFDM technology used in 802.11a/g/n falls in to an area called spread spectrum-like. Wireless technology standards are changing as testing verifies the capabilities and features of each product.

If two wireless signals are sent at the same time running on the same channel, they may collide and interfere with one another, requiring signals to be resent and ultimately slowing down the associated wireless process. Signals are literally floating through the air. These have the ability to bounce and redirect themselves, as well as to absorb themselves into their physical surroundings such as walls, floors, trees and the like.

Service Set Identifiers (SSID)

In order to set up a wireless network for proper functionality, there are several required elements. These will vary depending on the level of security required for the network. There are two types of networks and they are referred to as a Basic Service Set (BSS) or an Independent Basic Service Set (IBSS). A BSS network consists of an access point or wireless router as well as some client devices. An IBSS network consists of a group of clients connected to one another. All networks will have an SSID. This ensures that traffic between radios, whether an AP or client device, can be directed to the proper destination. On power-up, clients (such as a laptop) are typically looking for a network with a particular name. Some clients can be configured to look for a network with only one name; some clients like the Windows-XP client can be configured to connect to a variety of networks if the appropriate parameters have been configured in the utility. By default, the SSID is advertised by the AP in the beacon frame and is visible to most any client utility or network monitoring tool. Some network administrators restrict the advertising of the SSID or do not allow a client that does not know the name of the SSID to connect. When enabling this feature, care must be taken to ensure that the clients can tolerate this condition. Not all clients can connect to networks that do not advertise their SSID, even if it is known and programmed into the client. Current enterprise class AP's can have multiple SSIDs which allow traffic and VLAN segmentation right to the edge of the network.

The AP will also need a channel on which to operate. This channel will be dependent on whether it is operating in the 2.4 or 5.8 GHz band. Some APs have an option to look for the least congested channel, but in most enterprise networks the administrator would plan out the channels. The clients will scan all channels for the SSID and attempt to connect on the channel where the best signal is received. This scanning can be done in two ways. One is a passive scan where the client simply looks at the beacon frames on the channels and the second is by sending probe request frames to APs that it sees in the beacon frames and analyzing the information received in the probe response frame. The way in which a client accomplishes this is left to the vendor. Not all clients do this in the same way. Once the client has completed the scan it will send a probe request frame if it has not yet sent the probe request. Upon receiving a probe response from the AP and processing what information it has gleaned from the beacon frame and the probe response frame, it determines if anything in these frames would prevent it from joining the network. If nothing will prevent it from joining the network, it will send an authentication frame.

Figure 1 – Basic Service Set (SAIT, Glen Kathler)

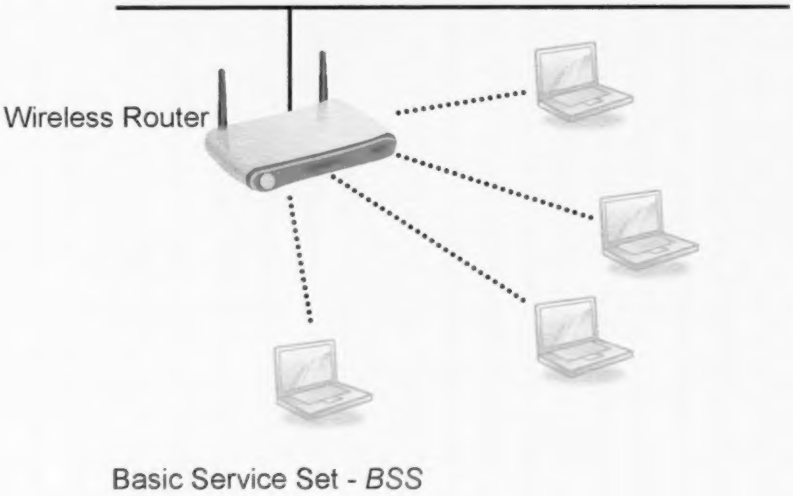
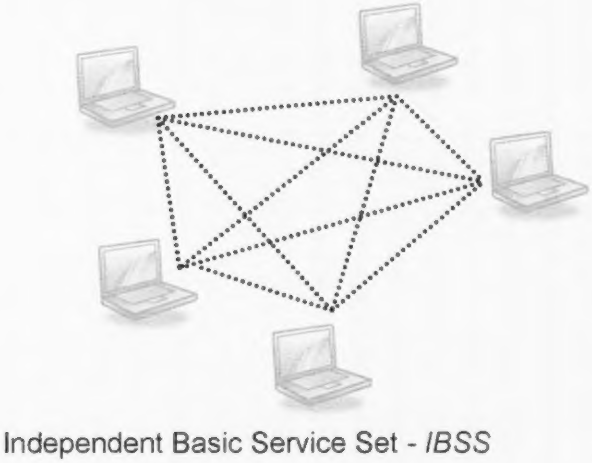

Wireless Router
Basic Service Set - *BSS*

Figure 2 – Independent Basic Service Set (SAIT, Glen Kathler)


Independent Basic Service Set - *IBSS*

Authentication and Association

This authentication process has nothing to do with the user of the device. The authentication just confirms that all layer 2 processes match between the client radio and the AP radio. The authentication response frame from the AP will indicate to the client whether it was successful in the authentication process.

Once authentication is complete, the next step is association, so the client sends an association frame and the association response frame from the AP will indicate the success or failure of the process. Assuming a successful association to the AP if there was no 802.1X mechanism enabled, the client would be able to gain access to network resources including DHCP, Internet, and so on. If an 802.1X mechanism was enabled, the client would then need to complete the user authentication before network resources could be accessed.

Once a wireless client recognizes an AP or device transmitting beacon frames, it will attempt to authenticate with it. This authentication process is not to be confused with a user authentication that takes place prior to gaining access to the networks resources, but simply a layer 1 authentication. If the layer 1 setting matches, which in the simplest form would be the Service Set ID (SSID), an exchange of frames consisting of beacon frames, probe request and probe response frames then takes place. An authentication frame exchange then takes place. If this is successful, the client and AP proceed to the association process.

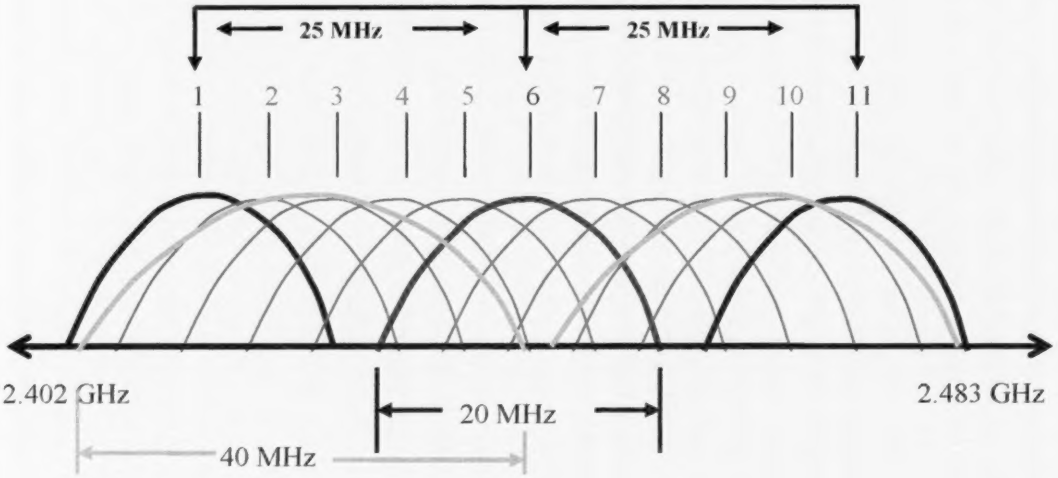
At this stage the client device typically scans all channels to see if the SSID it has discovered is available on any other channels. If so, it will make some signal strength measurements and attempt to associate with the AP with the strongest signal. A client can theoretically be authenticated to multiple APs but associated to only one. The association frame exchange takes place with the AP of the client's choice. In the 802.11e or QoS versions, the client will make this decision based on additional information related to how busy the AP is how much traffic there is on a particular AP. The first frame exchange is the probe request and probe response. This ensures that both devices are capable of the pending association. The client then proceeds with the authentication request, once the authentication response is received. The client reads the response for an accept indication, and it will then move on to the association request/response exchange. If this is successful, the client is allowed access to network resources or proceeds to some form of EAP authentication, if required.

Channels

The channels available for use in the various frequency bands and in conjunction with the different standards can be somewhat confusing. In the 2.4 GHz band there are 11 channels that can be used in North America. However they cannot all be used at the same time in the same location in an 802.11b or g network without interfering with one another. Channel 1, for example, is 2.412 GHz and channel 2 is 2.417 GHz, a channel spacing of 5 MHz. However, an 802.11b or g system requires a minimum RF bandwidth of ≈22 MHz. The Figure 3 shows the approximate RF bandwidth required for each channel.

The channel setup for 802.11n is a little more complex in the 2.4 GHz band. There are two channels for use, one called a wide channel (40MHz) and one a narrow channel (20 MHz). The wide channel is for the n-capable radios and the narrow channel is for any b/g radios that may still be present on the system. In a HT- greenfield system these would be disallowed or disabled. The wide channel can be any channel number from 3 to 9 with the narrow channel numbered either two above or two below the wide channel. For example, choosing to set the wide channel on channel 3 would make the narrow channel either channel 1 or channel 5. There can theoretically be two non-interfering 802.11n systems co-located in the 2.4 GHz band with the wide channels set to 3 and 9 and the narrow channels set to 1 and 11 respectively. Typical deployments in the 2.4 GHz band utilize 802.11n with a 20 MHz channel to still allow three non-interfering APs, which allows sufficient channels for roaming applications. The wide channel is readily utilized in the 5.8 GHz spectrum where there are 19 non-interfering channels available.

Figure 3 – Channels (SAIT, Glen Kathler)

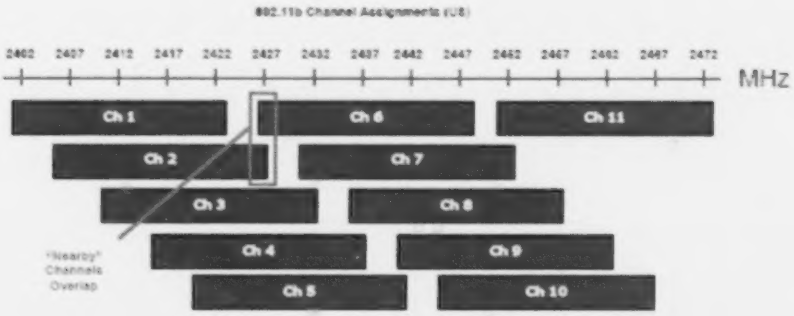


The 5.8 GHz UNII band has been structured differently and the channel plan and bandwidth allocations have been designed with these applications in mind. The channels are each 20 MHz wide and the center frequency of each is separated by 20 MHz allowing adjacent channel numbers to be used. For example, the UNII-1 band between 5.15 GHz and 5.25 GHz has 4 non-interfering channels allocated. These are channels 36, 40, 44 and 48. With the UNII-2E band being added recently, there are 19 non-interfering channels available for indoor 802.11a technology. UNII-1,2 and 2E bands are for indoor point to multipoint applications. There is an allowance for point-to-point applications in these bands; however the EIRP limits are the same as for point-to-multipoint. The UNII-3 band is only for use for outdoor point-to-point applications. The standard allows for different EIRP limits in each band to support their applications. The table below describes the UNII bands.

Table 2 - Channels and Bands (SAIT, Glen Kathler)

Band (GHz)	Channels	Channel Numbers
UNII-1 (5.15 - 5.25)	4	36,40,44,48
UNII-2 (5.25 - 5.35)	4	52,56,60,64
UNII-2E (5.470 - 5.725)	11	100,104,108,112,116,120,124,128, 132,136,140
UNII-3 (5.725 - 5.825)	4	149,153,157,161

Figure 4 – Channel Assignment (SAIT, Glen Kathler)



Collision Management

The radio channel is a shared medium. A collision occurs when two wireless waves of the same type (either infrared, DSSS or FHSS) and frequency (i.e. on the same channel) intercept in mid-air. The colliding signals corrupt each other. Wireless networks must deal with the possibility of collisions just as wired networks do. However, the devices on the wireless network have no capability to determine if a collision has actually taken place. A carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) mechanism governs how the radio channel can be used. All 802.11 devices are half-duplex in nature and thus cannot listen and transmit at the same time. Because of this design criteria, the devices must attempt to avoid collisions altogether. Due to the mobile nature of a wireless network, there will be times when not all clients associated to a single AP can hear each other. This creates opportunities for collisions and the protocol behind CSMA/CA can help mitigate this. Some of the main differences between an 802.11 network and that of a typical wired 802.3 Ethernet network are:

- All frames carrying data on the 802.11 network must be acknowledged;
- Without the positive acknowledgement of a data frame, the sender of the frame assumes a collision and resends the frame;
- The mechanism also provides a variety of mandatory wait times that all radio devices must use between the delivery of frames as well as when a device is waiting for the network to become available; and
- The mechanism also invokes a *random back-off timer* when the network is in use to ensure that all stations waiting for network access do so in an as orderly fashion as possible.

This process is what adds the majority of the reduction in throughput to the network. The balance of the reduction in throughput comes from the control and management frames required on the wireless network.

Several extensions of this mechanism exist, which are RTS/CTS as well as fragmentation. These are primarily used as optimization techniques for a network administrator in a network where more collisions and interference are present than normal.

There are two carrier sense mechanisms. One is a *physical carrier sense* which checks the Received Signal Strength Indication (RSSI). This determines if there are stations currently transmitting on the network as well as the ratio of the signal to the background noise on the channel. The other is a *virtual carrier sense* which uses a process called the Network Allocation Vector (NAV). This field is derived from the frames traversing the network which contain a duration field. This is data filled by the transmitting station to alert stations listening to the network as to how much time the network will be reserved for the current frame transaction. Once the NAV has been filled with a time value from the received duration field, the device immediately begins counting down until the NAV reaches zero. Only when the NAV is zero and the RSSI indicates the channel is clear can a wireless devices gain access to the channel.

Inter-frame Spacing

These spaces are integral to the operation of a wireless network. There are primarily three of these spaces that affect the use of the wireless network.

The Short Inter-frame Space (SIFS) lasts 10 µseconds. This space is mandatory between data frames and the required acknowledgement (ACK) frame. It is used following a Request-to-Send (RTS) frame that is used to reserve the network for a specific frame transaction. It is also used in a Clear-to-Send (CTS) frame which is the response to a RTS frame and allows this RTS/CTS transaction to occur without other stations gaining access to the network. This space is the shortest of all the inter-frame spaces.

The second of the inter-frame spaces in use is the Distributed Coordination Function Inter-frame Space (DIFS). The DIFS lasts 50 µseconds and is the time that must expire before any device can even begin to contend for the network.

The third space of concern is referred to as the slot time and is 20 µseconds in duration. This is used during the random back-off timer when the network is in use. The station selects a random number and multiplies this against the slot time to determine how long the network must be idle before it can contend for the network. This is also the section of the standard that has been modified by 802.11e QoS functionality. By altering these values, various types of media frames such as voice and video can achieve a higher priority than that for best-effort data, management and control frames.

With the advent of 802.11n and a variety of priorities being assigned to the different types of traffic, the standards now include the ability for a client to send multiple frames prior to requiring an ACK. This removes some of the overhead traffic that had a great impact on throughput in the original 802.11 standards. In fact overhead has been reduced by 10% in an 802.11n deployment. With the highest data rate of 802.11n (current hardware capabilities) set to 300 Mb/s, it boosts the throughput from about 138 Mb/s to 168 Mb/s. These rates are only achieved in the area of coverage immediately surrounding the AP where the data rate MCS15 can be used.

Figure 5 – Interframe Spacing (SAIT, Glen Kathler)

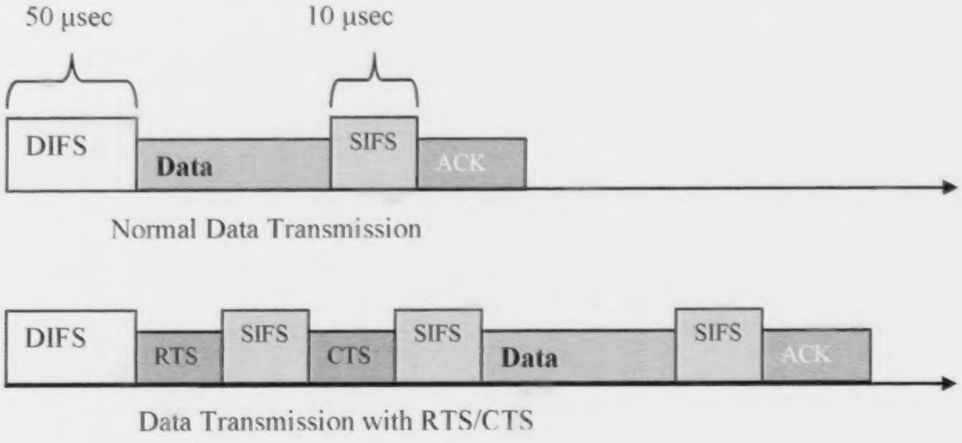
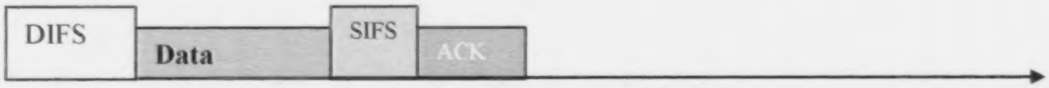
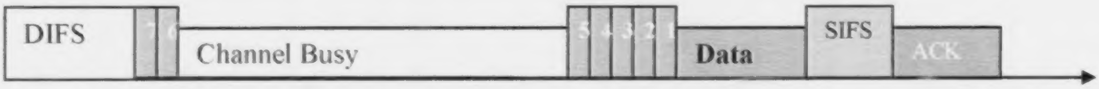


Figure 6 – Interframe Spacing 2 (SAIT, Glen Kathler)



Normal Data Transmission Station 1 Back-off time expired



Normal Data Transmission Station 2 Back-off counter halted during Station1 transmission (slots not shown to scale)

Power

The operator of a wireless network needs to ensure that all network devices operate within the Industry Canada regulations for Effective Isotropic Radiated Power (EIRP). This is how much power the respective device and its antenna system are radiating into free space. Industry Canada governs the use and specifications of all radio spectrum, even though the 802.11 bands are license-free. The other item that is regulated is the Intentional Radiator (IR), the amount of RF energy that is being fed into the antenna. The IR power limit is set at 1 Watt or 30 dBm.

Wireless networks are typically categorized into two families - one is a point-to-point configuration and the other a point-to-multipoint configuration. The point-to-point configuration is typically used in the example of a wireless bridge link. This is where two sections of network need connectivity and the solution chosen is a wireless bridge. Here the two wireless devices use a very directional, narrow beam width antennae and are allowed a higher EIRP than the point-to-multipoint system. If the antennae chosen are of an omni-directional type (those with a radiation pattern of 360°) the system is automatically governed by the point-to-multipoint rules. The maximum allowed EIRP for a point-to-multipoint system is 36 dBm or 4 watts.

Using the maximum IR power of 30 dBm and the maximum allowed EIRP of 36 dBm, this would allow a maximum antenna gain of 36 dBm – 30 dBm = 6 dBi. The gain of an antenna which is passive is measured with respect to a theoretical antenna (the isotropic radiator) therefore the term dBi. For every additional 3dBi of additional antenna gain added to this system, the IR power must be reduced by 3dB below the initial +30 dBm. Antenna manufacturers typically build their antennae in multiples of 3 dBi of gain. So these are the rules for point-to-multipoint systems.

If a system is determined to be a point-to-point system with very directional, narrow beam width antennae, then the rules are slightly different. In this case, for every additional 3Bi of antenna gain above the initial 6 dBi the power of the IR must be reduced by 1dB from the initial +30 dBm. This allows point-to-point to be installed that can cover distances in the 30 to 50 km range depending on the antennae and IR power chosen. There is some additional relaxation of these rules in the UNII-3 band 5.725 – 5.825 GHz. This band, which is primarily for point-to-point links, allows antennae with a directional gain up to 23 dBi before any reduction in IR power is required. This allows point-to-point links an EIRP of 200 Watts.

2.2 Wireless Security Standards

Wireless network traffic flows in an open medium, the air interface, and must be considered insecure. A network administrator must be aware of the types of security risks there are, as well as some of the solutions available to mitigate those risks. Some of the attacks against a wireless network cannot be prevented and only effective monitoring of the network and proper responses will reduce the risk associated with the wireless portion of a network. In most cases, the role of wireless in the network is to create access to a network already in place or the Internet. As such, some form of authentication and segmentation is required to manage who can access specific network resources. As wireless technology is introduced into enterprises where security is mandatory, wireless traffic needs to be secure.

CIA is a common acronym to describe the requirements of a wireless security solution:

C	Is the data on the network being kept as **Confidential** as it needs to be?
I	Is the network maintaining its **Integrity**?
A	Are the users on the network who they are supposed to be? Have they been **Authenticated**?

First generation 802.11 wireless devices were expensive, scarce and users were not particularly concerned with security. Wired Equivalent Privacy (WEP) was incorporated into the original standard as it was thought to provide just that.

Security in all networks is woven into the security policy of the enterprise. How sensitive is the data on the network? What are the risks if data is compromised? What defines acceptable use? As well, it is usually combined with an authentication scheme to provide not only authorized use but effective encryption. Most of the existing wired network user authentication methods can be leveraged over a wireless network.

Packet Encryption and Authentication

Many different methods are available for authentication, encryption and a combination of the two. The sections that follow briefly describe these methods.

EAP and 802.1X Authentication Protocols

Wireless security has evolved to use additional, more robust methods. APs can use a variety of authentication methods that leverage external authentication and authorization servers and their user databases. The Extensible Authentication Protocol (EAP) forms the basis for many wireless security methods, most of which have similar acronyms, such as EAP, PEAP, and LEAP. So many different methods exist that it is becoming confusing about what they are and what they do.

Comparison of EAP Methods

Table 3 - Comparison of EAP Methods (SAIT, Glen Kathler)

Authentication Protocol -->	EAP-MD5	EAP - LEAP	EAP- TLS	TTLS (EAP-MSCHAPv 2)	PEAP (EAP-MSCHAPv 2)	PEAP (EAP-TLS)	PEAP (EAP-GTC)	EAP-FAST
802.1X Authentication Characteristics								
Client certificates	No	No	Yes	No	No	Yes	No	No
Server certificates	No	No	Yes	Yes	Yes	Yes	Yes	No
Client Password	No	Yes	N/A	Yes	Yes	No	Yes	Yes
Security Level	Weak	Weak (depends on password strength)	Strong	Strong	Strong	Strong	Strong	Strong (if Phase 0 is secure)
Mutual Authentication	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Compatible with WPA	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Tunnelled Authentication	No	No	Yes	Yes	Yes	Yes	Yes	Yes
Encryption key management	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes

802.1X

Upon detection of the new wireless client, the supplicant, the port on the switch, the authenticator, is enabled and set to the unauthorized state. In this state, only 802.1X authentication traffic will be allowed. Other traffic, such as DHCP and HTTP, will be blocked at the data link layer. The authenticator will send out the EAP-Request identity to the supplicant, the supplicant will then send out the EAP-response packet that the authenticator will forward to the authenticating server, usually a RADIUS server (Remote Authentication Dial In User Service). The authenticating server can accept or reject the EAP-Request. If it accepts the request, the authenticator will set the port to the authorized mode and normal traffic such as HTTP will be allowed. When the supplicant logs off, an EAP-logoff message is sent to the authenticator. The authenticator then sets the port to the unauthorized state, once again blocking all non-EAP traffic.

In the WLAN world, 802.1X by itself is a port-based access control, a flexible authorization scheme that can work with WPA, WPA2 or 802.11i technologies. It is typically combined with an authentication protocol, and as a pair they provide a secure authentication and encryption key rotation mechanism.

Not all hardware supports 801.1X. You may be required to upgrade Network Interface Cards (NICs), APs, Switches or other hardware to implement 802.1X.

WLAN Authentication and Encryption

In 802.11 networks, clients can authenticate with an AP using many methods. The following are some of the most common means of connecting to a WLAN. It is worth noting that the level of security provided varies under the different methods. These methods are listed in order of the level of security which they provide, starting with the oldest and generally accepted as least secure.

Open authentication

Open authentication is usually the default, and offers no client screening whatsoever. Any client is permitted to join the network without presenting any credentials. In effect, the SSID is the only credential that is required. Although this makes life easier, it does not do much to control access to the WLAN. In addition, open authentication does not provide a means to encrypt data sent over the WLAN.

Status: This is insecure and not suitable for K-12 school environments.

Shared Authentication

The same secret key is statically defined on the client and the AP. If the keys match, the client is permitted to have access. Notice that the authentication process in these two methods stops at the AP. In other words, the AP has enough information on its own to independently determine which clients can or cannot have access.

Shared authentication uses a long Wireless Equivalence Protocol (WEP) key that is stored on the client and the AP. When a client wants to join the WLAN, the AP presents it with a challenge phrase. The client must use the challenge phrase and the WEP key to compute a value that can be shared publicly. That value is sent back to the AP. The AP uses its own WEP key to compute a similar value. If the two values are identical, the client is authenticated.

When shared key authentication (commonly called *static WEP keys*) is used, the WEP key also serves as an encryption key. As each packet is sent over the WLAN, its contents and the WEP key are fed into a cryptographic process. When the packet is received at the far end, the contents are unencrypted using the same WEP key.

As expected, a static key persists for a very long time, until someone manually reconfigures a new key. The longer a key remains in use, the longer malicious users can gather data derived from it and eventually reverse-engineer the key. It is commonly known that static WEP keys can be broken.

Status: This is insecure and not suitable for K-12 school environments.

Wired Equivalent Privacy (WEP)

Wired Equivalent Privacy was incorporated into the original standard as a means to encrypt the traffic on the network. From the wireless vendor's perspective, it was easy to implement, did not require much CPU power to encrypt and decrypt traffic, exportable, self-synchronizing and used a relatively strong cipher. The weakness that has been exploited is related to the fact that a static key entered in both the AP and the client is required. This key is only changed manually, typically by an administrator of the devices and must match on both devices. With these static keys being used to encrypt traffic on the network, an intruder can capture encrypted traffic and then run the traffic against an encryption cracking software or now even orchestrate a live encryption key cracking event on a network that employs this security mechanism.

Status: This choice is vulnerable. Avoid use as the only means of WLAN security for school networks because vulnerabilities and cracking tools have been published. If WEP must be used, it should be configured for 128-bit encryption, and passwords must have a high degree of entropy.

Status: Overall, this is insecure and not suitable for K-12 school environments.

Wi-Fi Protected Access (WPA)

WPA was initially a stop-gap measure implemented by the Wi-Fi Alliance to provide an interim security option during the time that 802.11i was under development. It actually repairs the primary weakness in WEP with a mechanism to rotate the encryption keys periodically and removes any requirements from the administrator or user to manually enter an encryption key. It also allows for each device to use a unique encryption key rather than sharing the same key with all the other users on the AP. The two methods of creating the key to be used for encryption are first of all a passphrase method. This method once again requires a manual entering of an 8 to 63 character passphrase in both the AP and the client. The passphrase must match in all devices using this AP. As a client connects to the AP, the client and AP go through a process called a four-way handshake to derive the encryption key for that client. The passphrase then is the weak link in this method and there are already software tools that can be used to derive the passphrase from a captured four -way handshake. This can be mitigated to some degree by a strong passphrase. WPA offers the following wireless LAN security measures:

- Client authentication using 802.1X or a pre-shared key;
- Mutual client-server authentication;
- Data privacy using Temporal Key Integrity Protocol (TKIP); and
- Data integrity using Message Integrity Check (MIC).

TKIP leverages existing WEP encryption hardware that is embedded in wireless clients and APs. The WEP encryption process remains the same, but the WEP keys are generated much more frequently than the periodic re-authentications that occur with EAP (Extensible Authentication Protocol, defined further in following pages) based authentication methods. In fact, TKIP generates new WEP keys on a per-packet basis. An initial key is built as a client authenticates (or re-authenticates) with the EAP-based method. That key is formed by mixing the MAC address of the transmitter (the client or the AP) with a sequence number. Each time a packet is sent, the WEP key is incrementally updated. Once the client is forced to re-authenticate, an entirely new WEP key is built and the per-packet process repeats. WPA can use a pre-shared key for authentication if external authentication servers are not used or required. In that case, the pre-shared key is used only during the mutual authentication between the client and the AP. Data privacy or encryption does not use that pre-shared key at all. Instead, TKIP takes care of the rapid encryption key rotation for WEP encryption. The MIC process is used to generate a "fingerprint" for each packet sent over the wireless network. If the fingerprint is made just before the packet is sent, the same fingerprint should match the packet contents once the packet is received. Why bother fingerprinting packets in the first place? When packets are sent over the air, they can be intercepted, modified, and re-sent—something that should never be allowed to happen. Fingerprinting is a way to protect the integrity of the data as it travels across a network. For each packet, MIC generates a hash code (key), or a complex calculation that can only be generated in one direction. The MIC key uses the original unencrypted packet contents and the source and destination MAC addresses in its calculation, so that these values cannot be tampered with along the way.

Status: The recommended usage for this type of encryption is in the small office/home office (SOHO) and consumer use environment.

WPA has been embedded into the 802.11 standard for the last three revisions, covering a period of six years. All equipment manufactured since its first release support WPA. Some vendors released WPA2 products somewhat later as the actual hardware in the radio needed upgrading to allow this improved encryption process to be used. Its official name is actually 802.11i.

Wi-Fi Protected Access Version 2 (WPA2)

WPA2 is based on the final 802.11i standard. WPA2 goes several steps beyond WPA with its security measures. For data encryption, the Advanced Encryption Standard (AES) is used.

AES is a robust and scalable method that has been adopted by the National Institute of Standards and Technology (NIST, www.nist.gov) for use in the U.S. government organizations. TKIP is still supported for data encryption, for backward compatibility with WPA. With WPA and other EAP-based authentication methods, a wireless client has to authenticate at each AP it visits. If a client is mobile, moving from AP to AP, such as a student with a tablet PC walking throughout the school requiring constant connectivity to the WLAN, the continuing authentication process can become cumbersome. WPA2 solves this problem by using Proactive Key Caching (PKC). A client authenticates just once, at the first AP it encounters. As long as other APs visited support WPA2 and are configured as one logical group, the cached authentication and keys are passed automatically.

Status: Superior security over WPA and the minimum recommended level of WLAN security for a K-12 school environment.

Not all hardware supports WPA2. You may be required to upgrade Network Interface Cards (NICs), APs and/or other hardware to migrate from WPA to WPA2.

Personal vs. Enterprise in WPA and WPA2

Within the above described WPA and WPA2 authentication/encryption methods, there are two further types. The first type is known as personal and the other is referred to as enterprise. The primary difference between these two types is that personal does not use EAP or a server such as RADIUS to authenticate users. Personal stores all security settings within the APs themselves. Enterprise uses EAP to facilitate authentication with an authentication server such as RADIUS. Variations of these methods are described next.

WPA personal mode and WPA2 personal mode do not use an EAP type and a managed authentication server such as RADIUS. Instead, they work from a static list of keys stored in the access point. Avoid use on company networks because vulnerabilities and cracking tools have been published. If PSK must be used, passwords must have a high degree of entropy.

In an enterprise environment, some flavour of authentication is needed whereby users are required to authenticate to a Server, an Active directory, RADIUS, LDAP data base or some other type of resource that maintains the users and their credentials. This eliminates the weakness of the passphrase in WPA-PSK. There are three elements of this process - supplicant (client), authenticator (AP) and the authentication server (AS). In some enterprise APs, the authentication server may reside in the AP. Typically, once that process is complete the server and the client determine the encryption key for that user and that specific session. The AS then sends the encryption key to the authenticator for use in that specific session. WPA still uses a WEP key, but each client has their own encryption key. WPA2 assigns a unique key for each client; however, it uses the AES encryption mechanism.

Both WPA/WPA2 personal and enterprise are among the strongest level of security available today.

Use enterprise over personal for its superior centralized control and management of user authentication credentials.

In addition to the previously described authentication and encryption methods, it has become commonplace to add VPN technology as an additional layer of security for mobile devices.

If students are taking laptops off school grounds and require access to the Internet or other digital resources, VPN technology is highly recommended. It will allow you to control and monitor content while protecting students. See Chapter 4 for more details.

VPN technology has existed since the days of remote access via dial-in modem to the corporate network. This technology can be implemented in wireless networks as well. It can provide encryption, tunnelling and security when a wireless client gains access to an unsecured network, such as a local hotspot. Prior to the client gaining access back to his corporate network, he is required to authenticate in some manner against a VPN concentrator at the corporate headquarters. A tunnel and encryption can then be setup between the concentrator and the client to secure the transport of packets between them over an un-secure network such as a wireless connection. Some wireless routers are also capable of acting as the VPN concentrator or endpoint. This allows clients to establish a secure tunnel between itself and the wireless router.

Figure 7 – VPN Tunnel Between Client and Network VPN Concentrator

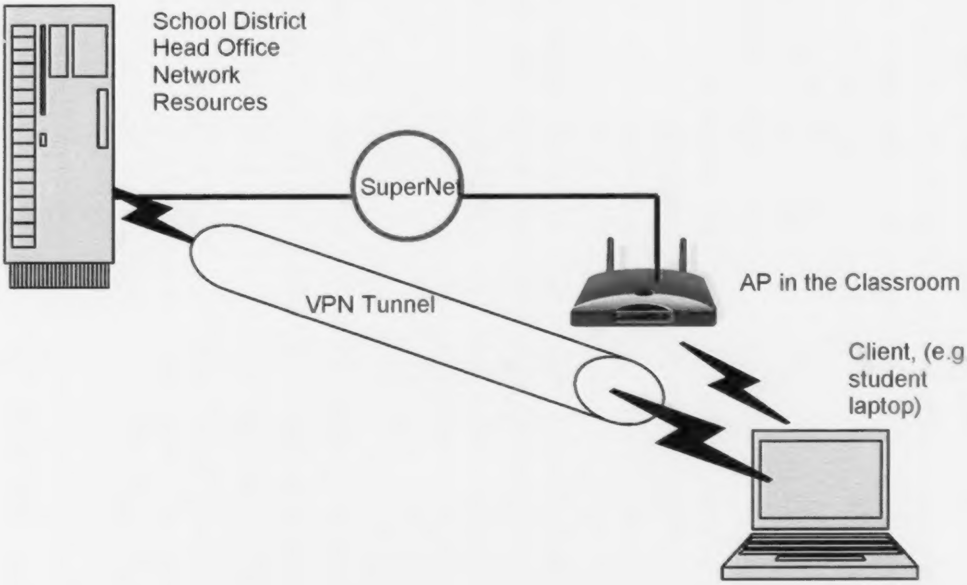
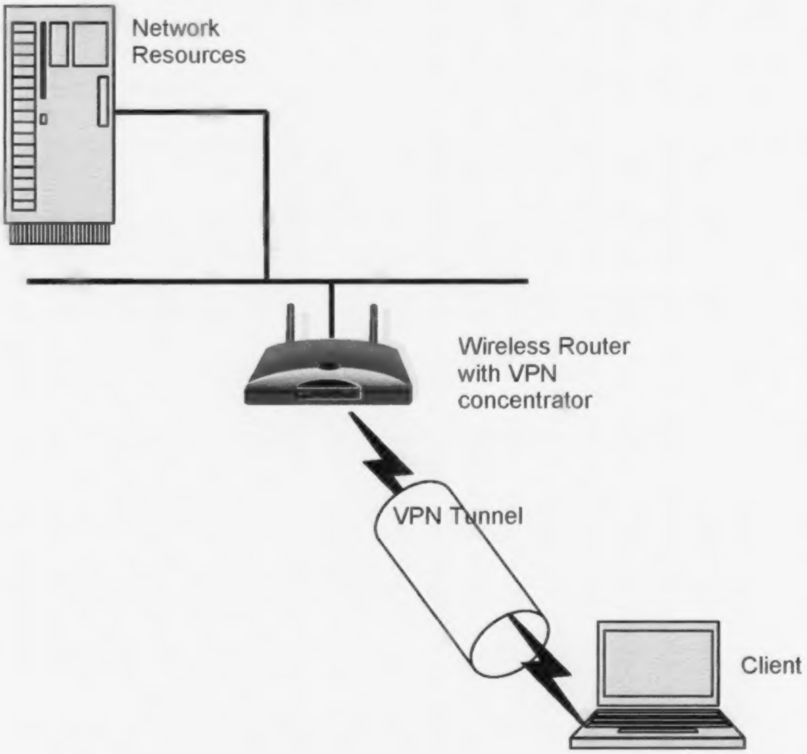


Figure 8 - Tunnel Between Client and Wireless Router


Network Resources
Wireless Router with VPN concentrator
VPN Tunnel
Client

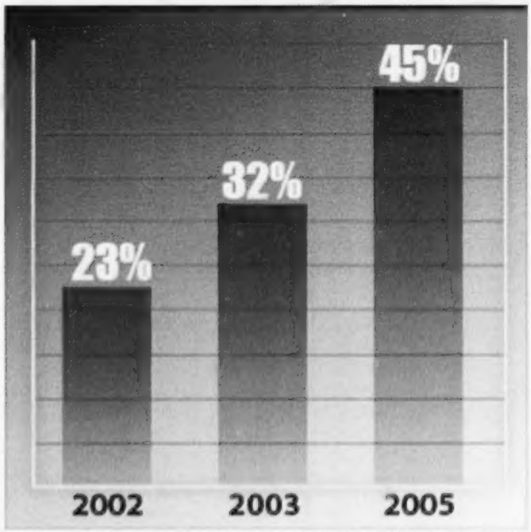
2.3 Overview of Wireless Market and Vendors

This section provides a snapshot of the wireless market today, including insight into the adoption of WLANs into K-12 schools. Information from several vendors is included, although this is not an endorsement of any particular vendor, whether they are listed or not.

Market Overview

A recently released American study on Internet access showed dramatic growth in wireless Internet access in public schools in 2005. All told, 45% of public schools in 2005 used some form of wireless Internet access, a growth of more than 40% over 2003, in which only 32% of public schools had wireless access.

Figure 9 – Use of Any Type of Wireless Internet Connection, 2002 – 2005 (NCES Survey 2006)



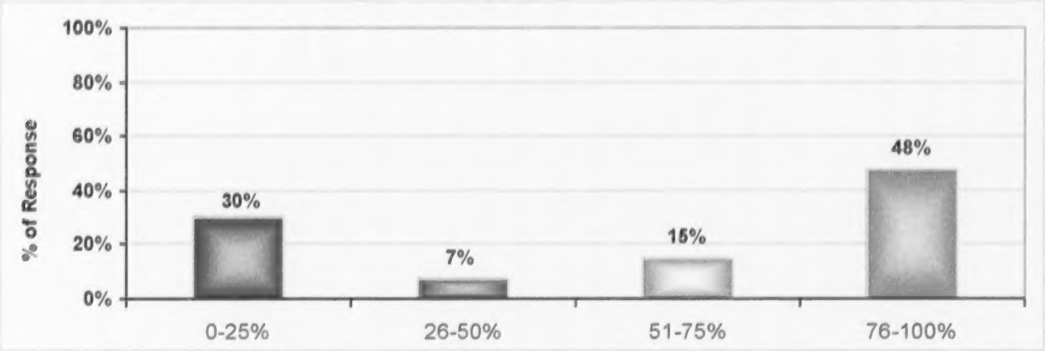
Source: NCES survey: Internet Access in U.S. Public Schools and Classrooms: 1994–2005, *published November 2006.*

In 2005, 45% of elementary schools had some sort of wireless Internet access, up from 29% in 2003. Secondary schools came in ahead of elementary schools at 48% in 2005, but the increase from 2003 was slighter, up just six points from 42%.

Alberta's Education System and Adoption of WLANs

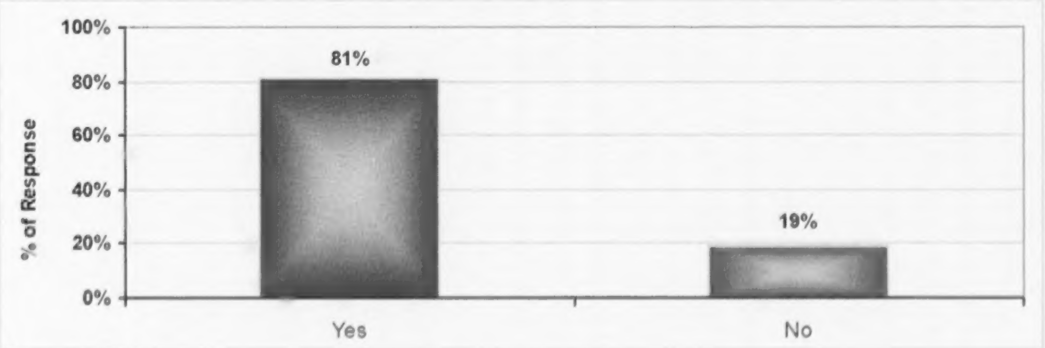
Wireless LAN adoption is growing in Alberta. In a 2010 survey of school authorities, 56% of participating school authorities offered wireless services and 81% responded they plan to increase the number of schools offering wireless.

Figure 10 – Percentage of School Authorities Reporting Proportions of Schools Offering Wireless Network Services



n=54, Source: QD5 and QA4
Note: Totals may not add to 100% due to rounding.

Figure 11 – Percentage of School Authorities Planning to Increase Number of Schools Offering Wireless by 2013



n=36, Source: QD6
Note: Totals may not add to 100% due to rounding.

The case studies in Appendix A provide for a summary of five school authorities' experiences with WLANs.

Market Description

WLANs are becoming a standard part of school networks. One of the biggest driving factors is one-to-one laptop learning initiatives delivering education to students with laptops, tablets, iPhones and other smart phones. There are a vast number of manufacturers, original equipment manufacturer (OEM) partners and resellers providing solutions in Canada today. The overwhelming trend for business customers, as well as K-12 schools, is moving toward APs with wireless controllers for WLAN architecture, also referred to as *thin* APs. However, small offices and schools continue to deploy fully functional stand-alone APs, also referred to as *thick* APs. The *thick* AP solution, for a coverage model soon becomes a capacity model which leads to a *thin* model. Some vendors allow their *thick* APs to be re-imaged to the *thin* model when the move to a controller based solution is needed.

If only planning for and deploying a small number of APs at any given school, thick APs can be a suitable solution. However, for larger deployments and scalable solutions with the most efficient remote, centralized management capabilities, *thin* AP solutions are becoming the standard.

Three key reasons for deploying wireless LANs are:

1. Increased productivity;
2. Broadening access areas where cost or physical barriers have limited traditional wired networks; and
3. Improved efficiency in specific processes.

Technically, WLANs are considered quite secure today, so long as they are correctly specified (i.e. optimal hardware and software for the specific application), configured and managed. Due to the adoption of IEEE standards and overall improvements to wireless technology, wireless is now being deployed behind firewalls instead of being an offshoot of the infrastructure, as it was in its infancy. The ability for a user to authenticate in the same fashion on a wired or wireless network makes the adoption by users seamless.

The manufacturer-specific security solutions offered have started to raise the wireless authentication framework as an issue that must be considered. However, lack of total interoperability is still a barrier to simple deployment. One of the biggest concerns is with the increased scope of network management, which often requires additional training for staff. With many school authorities that use their wireless networks primarily as a data network, thin AP solutions are agile enough to provide coverage if capacity becomes an issue. As these networks mature and more time sensitive applications such as VoIP use the wireless network, optimization and network management will become an even higher priority.

Previously, locations such as a branch office or an individual school site were identified as a network node. Now it is demanded that each and every device (used by employees, teachers or students) is identified as a node on a wired or wireless network. This is empowering IT departments to increase control and management right down to the desktop and application layer.

The enterprise WLAN infrastructure market is comprised of a great number of high and low-risk vendors with varied capabilities and company sizes. The best vendors will provide the widest array of options to tailor to a school authority's needs at the optimum price points. They will also offer flexible security and strong management tools. The good news is that the functions offered by the various vendors are narrowing to the core set described in this Guide.

Some vendors are stand-alone WLAN vendors that provide their technology as a non-invasive overlay to an existing wired network. Others possess a family of wired products that are highly integrated with the WLAN products. Where the latter exists, the best vendors have provided a single management console to control both network types.

Market Definition/Description

The WLAN infrastructure market consists of vendors that provide wireless IP networking solutions that conform to IEEE 802.11 standards through the Wi-Fi Alliance certification process. The core components of any WLAN vendor are:

1. Access Points (APs), each including radios and antennae
2. Controllers
3. Centralized Management Software

In very simple terms, APs are what the individual devices (laptops, PDAs or smart phones) connect to and controllers consolidate functions for centralized management software to perform updates and configuration of APs without the necessity of having to physically go to each and every AP.

All APs that contain a minimum of two radios that can act either as service link radios or as air sensors for security purposes. All radios are typically configurable across any of the bands in the aforementioned frequencies. Each radio supports multiple Basic Service Set Identifiers (BSSIDs). More advanced APs support the additional capability to use one of the radios for wireless backhaul and, in the more advanced systems, capability as a mesh networking vendor, however no "mesh-only" vendors are included in this section.

Vendors also provide a variety of antennae, from those that give simple diversity, to multiple input, multiple output (MIMO), to higher gain antennae that provide increased or focused coverage.

Virtually all incumbent wired LAN manufacturers have already launched WLAN products. Despite what the name says on the equipment itself, the actual solution is either their own or provided via an OEM partnership with another manufacturer.

Vendor Comparison

Table 4 – Original Vendor Comparison

Vendor	Controllers	Controlled APs	Stand alone APs	Firewall Appliance [1]	Firewall Software	Intrusion Detection	Wireless Network Management System
Alcatel-Lucent	Yes	Yes	No	Yes	No	Yes	Yes
Aruba Networks	Yes	Yes	No	Yes	No	Yes	Yes
Bluesocket	Yes	Yes	Yes	Yes [2]	No	Yes	Yes
Cisco Systems	Yes	Yes	Yes	Yes	No	Yes	Yes
Aerohive	No	Yes	No	No[3]	No	Yes	Yes
Enterasys Networks	Yes	Yes	Yes	Yes	No	Yes	Yes
Extricom	Yes	Yes	No	No	No	Yes	Yes
Extreme Networks	Yes	Yes	Yes	Yes	No	Yes	Yes
Brocade	Yes	Yes	Yes	Yes	No	Yes	Yes
Hewlett-Packard	Yes	Yes	Yes	Yes	No	Yes	Yes
Meru Networks	Yes	Yes	No	No	No	Yes	Yes
Motorola	Yes	Yes	Yes	Yes	No	Yes	Yes
Ruckus	Yes	Yes	No	No	No	Yes	Yes
Trapeze	Yes	Yes	No	Yes	No	Yes	Yes
Xirrus	No	Yes	Yes	No	No	Yes	Yes

---

[1] Some of these are security appliances now, which have firewall functions built in.

[2] Integrated into other appliances.

[3] Some firewall capability built into AP.

Chapter 3 Going Wireless Preparation and Planning

As with most critical decisions, proper planning is of the utmost importance. A WLAN deployment is no different. It can affect investment in other areas of the technology, including hardware (for laptops), software (operating systems for the laptops or other specific applications) and security (your existing and future network architecture, policies, and with students taking the laptops home, a new level of management requirements).

This section is meant to help in the decision making process of procuring, implementing and managing a wireless solution. It is intended to help you identify critical areas to be addressed in your processes of going one-to-one.

The most time and focus of any school authority's WLAN project should be invested in the planning stage.

3.1 First Steps

Setting Realistic Goals and Expectations

Goals of a WLAN in the K-12 Setting

WLANs are most inspiring in the context of what they will be used to accomplish. **How the system will be designed and implemented has everything to do with how it will be used**. A single AP running at 11Mb/s begins to see noticeable performance degradation at approximately 10 to 15 simultaneous users. This impacts the design and eventual success of the WLAN deployment.

The first step is a careful analysis of the intended uses of the wireless technology itself. Take into consideration the applications and uses of the WLAN equipment and architecture over the life of this investment. A typical life cycle of WLAN equipment is three to five years, so having a road map of its intended uses will help school authorities get the most out of this investment. Based on this analysis, a considered plan can be put in place. Once this information is available, an effective site survey can be conducted.

When defining WLAN architecture, focus on two distinct challenges:

1. Technology and educational policy requirements.
2. End-user requirements.

Because of increased adoption, more applications and services are being layered onto the WLAN. However, the number of applications utilizing wireless transport is not the only factor that is changing. The characteristics of the applications themselves are changing as well. Traditionally, WLANs in enterprises were intended only for data traffic. The key applications were typical business productivity tools such as e-mail, web browsers, calendaring tools, and messaging. These applications produce network traffic that is irregular and non-continuous. Periods with high network utilization are followed by periods of low network utilization, and the duration of both these periods is unpredictable. The applications load the network in bursts.

It is very likely in the lifespan of this WLAN infrastructure investment that a school authority's potential expansion of one-to-one initiatives and/or administration requirements may demand bandwidth-intensive and potentially latency-sensitive applications migrating onto the wireless medium.

Team, Roles and Responsibilities

As with any project plan, identifying the key individuals and clearly outlining the entire team's areas of responsibility is crucial. It is at this stage where the hard skills and actual individual capabilities must be honestly assessed. Ensuring that a district has the in-house capabilities to implement and manage all aspects of a WLAN will be a key to the success of a one-to-one initiative.

Specific One-to-One Initiative Considerations

Identifying which services and applications the WLAN must support is a key to building a robust, relevant, scalable and sustainable architecture. It is strongly urged to consider the following elements of any one-to-one initiative:

- Number of students in years 1 through 5 using the WLAN
- Types of applications being utilized
- Total bandwidth requirements
- Throughput requirements
- Security for laptops. Special attention should students be taking them home to access the Internet or other resources

3.2 Analysis

Use a 10:1 and not more than 15:1 Client-to-AP ratio for your budgeting analysis.
(Client = 1 student laptop or other device accessing the WLAN)

Immediate Scope and Future Scalability

The scope of WLAN deployment is one item that can easily be defined from the start. Whether defined to include all areas of every school in the school authority, or select classrooms and common areas of a few pilot schools, there is a boundary. Although the scope of WLAN deployment has a larger impact on the planning and implementation phases, it also plays a role in the architecture.

The architecture must formalize and document the coverage the WLAN provides. The formalization of the scope serves as a guide to ensure neither an under nor over-engineered WLAN solution. Under-engineering provides insufficient resources to the intended degree of service. Examples include inadequate coverage due to not deploying enough APs or failing to incorporate the proper IT security standards at the school authority level. Over-engineering is the inverse case. This happens when more resources are supplied than are needed to implement the desired solution. In this scenario, there is the potential for underestimating engineering resource allocation, and not meeting the project's financial budget target. An example of over-engineering is deploying too many APs. In this case it results in either overlapping coverage of APs or providing coverage in areas where there is no need for the WLAN access.

A key consideration when determining the scope of a WLAN is how it will be supported. There will be an increasing number of operational issues, including selecting a scalable strategy and platform for managing the WLAN's RF spectrum as well as potentially hundreds of APs and thousands of client devices. Leverage the scope as defined in the WLAN architecture as a planning tool. This structured approach makes it easier to determine how to offer support at the different levels of the fault resolution path and how to handle onsite resources for troubleshooting.

One of the key drivers of architecture will be whether devices owned by students and teachers, including laptops, tablets and smart phones, are allowed to connect to the WLAN. The number of connections must be managed closely, as well as the types, times and priority of applications running over the WLAN's infrastructure. With global sales of smart phones almost equalling the sales of laptops and tablets in 2010, it is estimated that the amount of smart phones accessing wireless networks will soon rival the laptop and tablet access.

Budget Requirements and Limitations

Budgets are always limiting. Their purpose is to provide a guide on the scope of what can be implemented. It is often times the *unforeseen* elements of many technology solutions that cause the most challenges. This Guide, in its entirety, is meant to help identify all aspects of implementing wireless into an IT strategy and bring today's best practices to light.

Be sure to include all aspects in a WLAN budget, including but not limited to:

1. Hardware (APs, Controllers, Switches, Devices, etc.); 2. Software one-time and subscription based charges (WLAN management, Security such as Anti-Virus, Anti-Spam, Anti-Spyware, Network Access Control, Intrusion Detection, Desktop management); 3. Maintenance and Support (in-house and/or out-sourced); 4. Training; and 5. Initial Setup.

SOHO versus Enterprise

The question of when to use an enterprise class instead of a small office/home office (SOHO) access points is a tricky one. Different manufacturers have varying features that separate an enterprise from a SOHO Wi-Fi solution. One must take into account the number of users in the network and their bandwidth needs. As a general rule, if an access point is expected to have more than ten clients connected to it at any one time, the wireless infrastructure may need enterprise class' increased robustness and additional features.

SOHO access points are commonly found in consumer retail stores. They are relatively inexpensive, have less scalability, and fewer features. Enterprise access points are more robust, scalable and expensive, which makes sense given that they are made to support more users with more varied needs.

Below is a table comparing SOHO and enterprise APs, which is not meant to be definitive by any means:

Table 5 – Comparing SOHO and Enterprise APs

Features	SOHO	Enterprise
Ease of deployment	Simple	Complex
Scalability	Less	More
Price	Cheaper	More expensive
Ease of management for multiple access points	Difficult	Easier (Centralized management)
Upgrade to new and faster radios	N/A	Available in some models
Power over Ethernet	N/A	Available in most models

Number of Ethernet ports	Less	More
Security	Weaker	More secure (AES, 3DES, IPSec layer 3 encryption)
Real Time Air Monitoring (Against Denial of Service attacks)	N/A	Available in some models
Adjustable Power Output (for signal strength)	Manual Control	Dynamic Control
Durability	Relatively less durable	Can operate in broader temperature ranges and environments with poorer air quality
WPA2 Authentication	Pre-shared passphrase or key (less secure)	Typically requires RADIUS server (more secure)
Support for multiple SSID	Not typically supported	Supported
VLAN support	Supported in higher end models	Supported
Wireless bridging	N/A	Supported
VPN	Supported in higher end models	Supported

Technology Selection

IEEE Standard 802.11 a/b/g/n

Today's Wi-Fi networks operate in one of two frequency ranges: 2.4 GHz and 5.8 GHz. 802.11b and 802.11g operate in the 2.4 GHz realm, while 802.11a sticks to the less-used 5.8 GHz band. 802.11b and 802.11g wireless implementations far outnumber 802.11a networks for a number of reasons. First, until 2003, 802.11a suffered from different regulations for the 5.8 GHz band, making it difficult for manufacturers to sell in some countries. Further, although 802.11a and 802.11g are relatively fast speed, 802.11a has a maximum range of 25 meters while 802.11g can range from 25 up to 75 meters, depending on environmental conditions and the WLANs' tolerance for slower speeds at the extremities of the coverage area. 802.11n can operate in both frequency ranges. This new standard is backward compatible with the legacy standards, however throughput is compromised with the admission of legacy clients onto the network. The throughput of the network mirrors the lowest standard allowed. Part of the migration to 802.11n is to determine at what point that legacy devices will not be allowed to access the network. At time of writing, the need to allow any 802.11b devices on the network has passed. Any 802.11b devices or clients should be replaced with a higher speed client. The trade-off to allow a few 802.11b devices against the overall throughput effect is significant.

While 802.11b and 802.11g support a good distance, the 2.4 GHz range is fairly cluttered and susceptible to interference from cordless phones, microwave ovens and other wireless networks, particularly in metropolitan areas. This means that schools that are close to office buildings or even homes may experience noise from these other WLANs. Each additional WLAN can create an environment that interferes with each other. For these reasons, schools may need to maintain 100% control of what authorized devices may connect to the WLAN. Consider rolling out an "802.11a-only" network. Most laptops come with multi-band cards that will simultaneously support all the 802.11 standards. Some controllers have the capability to load balance or shift traffic onto the 5.8 GHz network as well.

This will be very different for schools located in busy areas, close to other buildings compared to rural schools that are more isolated.

As identified by Edmonton Public Schools, implementing the frequency which will give you the least interference is likely 802.11a, with the migration to 802.11n and the ability to have only two non-interfering channels in the 2.4 GHz spectrum makes the 5.8 GHz spectrum even more appealing.

Hardware Vendor

Overall, vendor selection is one of the critical steps to a successful WLAN deployment. Each vendor has varying degrees of competitive differentiation which should be taken into account when procuring wireless solutions. Here are some general categories for assessing the right vendor for any school or school authority-wide implementation:

1. **Product Line**: A vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature set. Very simply, select the product that is best suited to the specific environment and requirements.
2. **Financial Analysis**: An assessment of the vendor's overall financial health, the financial and practical success of the business unit and the likelihood of the individual business unit to continue to invest in the product, continue offering the product and advancing the state of the art within the organization's portfolio of products. Note that WLAN vendors range in size from $10 million to $100 million to $90 billion in annual revenue.
3. **Experience and History**: Relationships, products and services/programs that enable customers to be successful with the selected products. Specifically, this includes the way customers receive technical support or account support. This can also include ancillary tools, support programs (and the quality thereof), availability of user groups and service-level agreements. Having implementations and references in the K-12 market is critical.
4. **Future, Scalability and Integration**: It is strongly advised to evaluate vendors on their ability to articulate and envision current and future market direction, innovation, customer needs and competitive forces. Direct, related, complementary and synergistic resources; expertise or capital for investment; consolidation; defensive or pre-emptive purposes related to innovation to ensure a constantly improving solution being offered. For example, a $100 million and a $90 billion vendor have dramatically different resources available to grow and address the WLAN business segment.
5. **Simplicity**: A clear, differentiated set of messages consistently communicated throughout the organization from public marketing and advertising information to customer programs. A vendor and their channel partners should make the buying experience painless and simple.
6. **Depth of Interaction and Relationship**: Vendors use direct and indirect sales, marketing, service, and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

Use a single vendor and centralized management software

This will increase security while optimizing the budget for maintenance and support. For example, with 50 APs on a network, and a security patch for a critical vulnerability is released, it is much easier to push that patch from a management console than it is to connect to individually apply it to each AP.

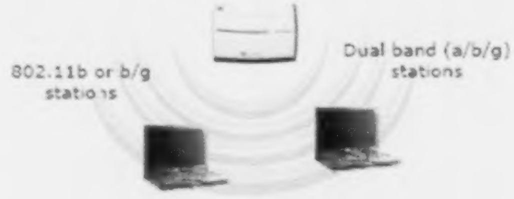
Dual-Band Radios and Dual Radio Access Points

802.11a/b/g/n multi-band (also referred to as dual-band) APs with two or more radios can simultaneously support both 2.4 GHz (802.11b/g) and 5GHz (802.11a) RF bands (whereas 802.11n can run on either 2.4GHz or 5GHz).

They offer backward compatibility to preserve existing investments along with a larger number of channels and increased throughput. A wireless station with a multi-band radio typically looks first for an 802.11a AP. If it cannot find one, it then scans for an 802.11g, and ultimately for an 802.11b. This process is controlled by the vendor firmware for the wireless client. Since this is typically a frequency choice, with the introduction of 802.11n the options can be similar.

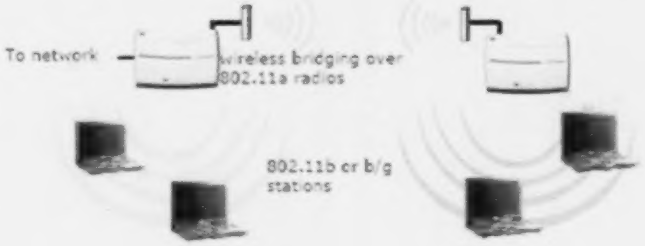
Multi-band APs are well suited to a wide range of network architectures. Further to the benefits of increased bandwidth, it is common to find deployments that use multi-band APs to segregate data types onto the different RF bands. The APs 802.11a radio can service wireless traffic from data clients (such as student laptops), while the 802.11b/g radio supports more time-sensitive traffic (such as staff and teacher usage) to create two separate RF networks.

Figure 12 – Simultaneous 802.11a and 802.11g Dual Radio Support (HP Procurve Networking, Planning a Wireless Network)



Alternatively, consider an application in which a multi-radio AP is deployed in a temporary or portable building – for example, in an outdoor portable classroom where there is no Ethernet connection. One radio (and associated antenna) is used for the backhaul link to communicate with a corresponding AP on the main school building, and the second radio (and associated antenna) is used to provide connectivity to users in the local wireless coverage area within the portable.

Figure 13 - Wireless Bridging Application (HP Procurve Networking, Planning a Wireless Network)



Most APs are now dual radios. For most enterprise applications, this provides the best scalability and throughput. With the ability for a client that begins a session on the 2.4 GHz radio, the controller can switch it to the 5.8 GHz radio to balance the load on the particular AP as necessary. This approach is particularly well suited to address areas of dense user coverage, such as adjoining classrooms, large lecture halls or common areas like cafeterias.

Tip: APs that have at least two radios can be used as a repeater to extend the coverage area.

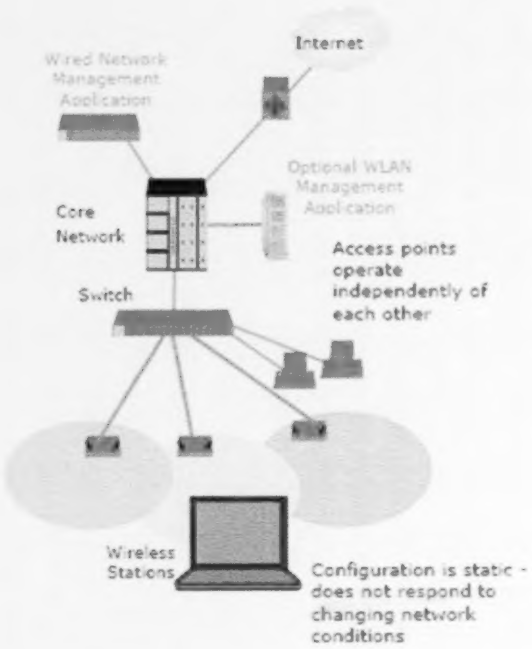
Centrally Coordinated versus Distributed AP Management

In determining which WLAN architecture to adopt, both distributed APs and centrally coordinated APs have benefits that are well suited to different environments. These architectures are also referred to as *thick* and *thin* respectively.

A wireless network based on standalone APs relies on the integrated functionality of each AP to enable wireless services, authentication and security. As shown in Figure 14, this network can be characterized as follows:

- All APs in the network operate independently of each other;
- Encryption and decryption is done at the AP;
- Each AP has its own configuration file;
- Larger networks normally rely on a Centralized Management Platform;
- The network configuration is static and does not respond to changing network conditions such as interfering rogue APs or failures of a neighbouring APs; and

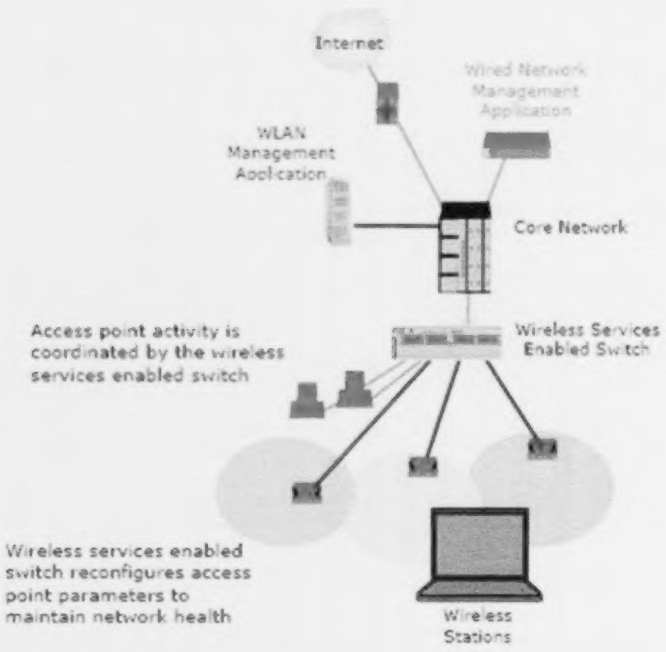
Figure 14 – Wireless Network Consisting of Stand Alone Access Points (HP Procurve Networking, Planning a Wireless Network)


Internet
Wired Network Management Application
Optional WLAN Management Application
Core Network
Switch
Access points operate independently of each other
Wireless Stations
Configuration is static - does not respond to changing network conditions

In a *coordinated* wireless network, thin APs have much simpler responsibilities. Most of the heavy lifting is performed by a centralized controller, also known as a wireless switch, which handles functions such as roaming, authentication, encryption/decryption, load balancing, RF monitoring, performance monitoring and location services. Because configuration is done once at the controller, adding additional radios to cover new classroom areas is as simple as plugging them in. As shown in Figure 15, this kind of network can be characterized as follows:

- AP activity is coordinated by a wireless centralized controller. Encryption/decryption and authentication are performed at the controller instead of at the individual APs;
- To maintain the health of the network, the controller can reconfigure AP parameters as needed, providing a self-healing WLAN (e.g. if an AP fails, neighbouring APs can increase signal strength to make up for the lost coverage of the failing AP);
- The wireless LAN controller performs tasks such as configuration control, load balancing, fault tolerance and network expansion;
- Redundancy can be provided through redundant controllers in separate locations that can assume control in the event of a switch or controller failure; and
- Supports PoE.

Figure 15 – A Centrally Controlled Wireless Network (HP Procurve Networking, Planning a Wireless Network)


Internet
Wired Network Management Application
WLAN Management Application
Core Network
Access point activity is coordinated by the wireless services enabled switch
Wireless Services Enabled Switch
Wireless services enabled switch reconfigures access point parameters to maintain network health
Wireless Stations

Both the distributed and centrally coordinated architectures have advantages and disadvantages, depending on the age of the wired infrastructure, deployment area, building architecture and types of applications supported. Regardless of approach, it is essential that the architecture provides a way to manage the WLAN efficiently and effectively.

A *distributed AP* WLAN is particularly well suited in environments where:

- There is a smaller, isolated wireless coverage area that requires only one or a few APs; and
- There is a need for wireless bridging from a main building to a remote portable or temporary building such as a portable classroom.

However, the operational overhead to manage and maintain a WLAN increases with the size of the WLAN deployment. Wireless LAN management tools that are generally proprietary to each vendor's associated hardware help simplify configuration and monitoring of the LAN, but the inherent "independence" of these APs presents a challenge in addressing security, configuration control, bandwidth predictability and reliability.

It is worth noting that when APs are first deployed, they must be configured. Such things as radio settings and authorized users must be added. Once WLANs are installed they are subject to frequent change as manufacturers update firmware and introduce new products; as new students are introduced and as security codes are updated. Each of these changes requires an administrator to physically or electronically touch each AP or device that connects to the WLAN. It is not cost effective to manage WLANs device by device, and hence if there will be more than just a few APs on the WLAN, opt for the centrally coordinated architecture.

A *centrally coordinated* WLAN is well suited to deployments where:

- There are one or more large wireless coverage areas that require multiple APs, possibly accompanied by several smaller isolated coverage areas;
- RF network self-healing is required; and
- A redundant stateful-failover solution is required.

Current trends indicate that centrally coordinated solutions are becoming the de facto standard. As wireless LAN deployments continue to grow larger, accommodating ever greater numbers of users, there will be an increasing demand to centrally manage a wide range of security, performance and configuration attributes as a single system from a single dashboard or software interface.

A centrally coordinated network offers many benefits, including:

- **Lower operational costs.** Centralized management facilitates ease of deployment and ongoing management. It is essential to minimize help desk calls and trouble tickets.
- **Greater availability.** In this architecture, it is easier to respond in real-time to changes in the network performance and spikes in user demand such as new students or temporary staff.
- **Better return on investment.** Fast client roaming and enhancements in Quality of Service provide traffic-sensitive applications with their required throughput.

As for all of their attractions in terms of performance, flexibility and affordability, WLANs also pose management challenges very different from those of wired networks. These challenges increase exponentially as WLANs grow in size, scope and complexity. The solution is to automate these management tasks by implementing best practice service level management processes and tools.

Emerging field tools are also complementing IT toolkits in filling the need to effectively manage the wireless environments. These tools provide the ability to detect rogue APs, determine security levels, determine where there are potential interference sources for wireless, such as cordless phones, and analyze wireless data.

There are many different ways to set up a wireless network. A certain density of APs is required to provide satisfactory network coverage and capacity, while many aspects of WLANs are analogous to wired LANs and should be managed in a consistent fashion, some aspects of wireless are unique. Wireless is a shared medium and, as such, requires careful planning for dynamic usage profiles and capacity variations.

Antennae Selection

Antennae allow for more efficient coverage for specific areas, and can help achieve desired coverage, capacity and bandwidth objectives. A higher-gain antenna focuses the radio's RF energy into a smaller area to achieve higher signal levels and a better Signal to Noise Ratio (SNR). This typically yields higher data rates over the area covered by the antenna. Selection of antennae must be done carefully as using higher gain antennae increases the footprint of the AP and reduce the per square foot capacity as adjacent APs need to be farther away.

For example, in a library with floor-to-ceiling wood or metal bookshelves requiring wireless network access for devices or laptops, deployment of external directional antennae to focus wireless coverage between each of these obstacles would be needed.

Antennae and Cabling

In very small networks, a consumer-grade wireless router with its default antenna is generally adequate. However, as a wireless network grows beyond a confined area, antenna choice becomes more important. Every different kind of antenna emits a unique radiation pattern, making certain antennae more suitable than others for specific applications. For example, a point-to-point wireless network connecting two buildings will usually not use the small omni-directional antennae shipping with most APs. Instead, specialized antennae that focus the transmission signal are used in order to achieve higher throughput and, sometimes, to lessen the scatter associated with less focused antennae. There are a large number of different types of antennae available for use with wireless networks. When considering antennae, also be mindful of the cables that connect antennae to your AP. The word "wireless" is a bit misleading. In reality, wireless APs typically need at least one cable—an Ethernet cable—in order to function, excluding APs configured as repeaters. However, if an AP is configured as a repeater the Ethernet cable typically provides only the PoE and the network portion of the interface is disabled depending on vendor implementation. Beyond repeaters, if APs do not support Power over Ethernet (PoE), plan for power outlets at each AP location.

This is one prime difference between the consumer-grade AP and the more expensive units designed for business, education and enterprise environments. The more expensive units generally support PoE. In addition to the network cable, be mindful of how much cabling is used to connect an AP to an external antenna. The longer cable, the more loss introduced in the transmission, resulting in lower EIRP and a smaller AP footprint.

Antennae Types

Three main types of antennae are commonly used in 802.11 wireless networking applications: parabolic grid, yagi and dipole. For more detailed information on antennae, refer to http://www.hp.com/rnd/pdfs/antenna_tech_brief.pdf.

Each antennae type is described in detail as follows:

Parabolic Grid

Perhaps the most powerful antenna for site-to-site applications is the parabolic grid antenna. A parabolic grid antenna can take many forms, ranging from something that looks like a satellite TV dish to one that has the same shape but is made of a wire grid instead of having a solid central core. This type of antenna is a unidirectional antenna, meaning that it transmits only in the direction in which the antenna is pointing.

Yagi

A yagi antenna is slightly less powerful than a parabolic grid, and it is suitable for site-to-site applications at lesser distances than a parabolic grid antenna. Like the parabolic grid, the yagi is also a unidirectional unit. A yagi antenna consists of a series of metal spokes radiating from a central core. The whole thing is covered by a tubular plastic housing called a radome, often concealing the actual antenna elements.

Dipole

A dipole is an omni-directional antenna, and its radiation pattern extends equally in the horizontal plane. Use a dipole antenna to support client connections rather than site-to-site applications. The standard antenna that ships with an AP is a dipole. It is normally rotated to be in the vertical position. As most client antennas are oriented vertically this gives the best signal between client and AP.

Antenna specifications

Understanding the different antenna types is only the beginning. Each antenna type has a number of specifications that directly affect how well it works. These specifications are antenna gain, beam width, loss, and radiation pattern.

Antenna gain

This is a measurement of how well the antenna focuses a signal. This is typically measured in dBi (decibels relative to isotropic radiator—a theoretically "perfect" antenna) and is based on decibels, which is a logarithmic measure of relative power. The dBi is computed by comparing the output of the antenna to a theoretical isotropic radiator (antenna) with a dBi of 0: the higher the dBi measurement, the higher the power level of the antenna.

Beam width

The beam width is the area radiating outward from the antenna where the signal within a specific angular distance is above the "half power" of the peak intensity of the antenna. The beam width is also loosely used to determine the antenna type. A parabolic grid antenna is a unidirectional antenna with a very low beam width, which means that it needs to be very carefully aimed at its partner in order to be effective. A vertical, omni-directional antenna has a very high horizontal beam width, which is why it is suitable for roaming client connections. However, its vertical beam width will be lower. In general, there is an inverse correlation between beam width and antenna gain, which means that the required accuracy for aligning antenna goes up as the gain increases because the beam width decreases.

Loss

Loss is an important factor when deploying a wireless network, especially at higher power levels. Loss occurs as a result of the signal traveling between the wireless AP and the antenna. Since APs are typically connected by a cable, there will always be loss. Loss can be minimized by using the appropriate type of cable in the minimum length required to make the connection.

Radiation pattern

Every antenna has a unique radiation pattern determined by its construction. This radiation pattern is a three-dimensional radiation field of the antenna's output. Some manufacturer's antenna supply sample radiation pattern specifications for their equipment. Use these specifications to determine how far the signal from a particular antenna can travel before becoming unusable. As a rule of thumb, a directional antenna has a conical pattern of coverage that radiates in the direction that the antenna is pointed, while an omni-directional antenna's area of coverage is shaped like a doughnut.

3.3 Project Plan

Timeframe

A modest estimate for a technically competent team of technicians to plan, communicate, survey, procure, configure, secure, test and report on a basic WLAN implementation (e.g. one school site with up to twenty APs) ranges from one to three calendar months. In Table 6 below is a sample project plan timeframe. This timeline can be adjusted (either shorter or longer) depending on the overall scope, size of the project team and the number of personnel involved in decision making.

Table 6 - Sample WLAN Project Plan (Network Integrators of Canada Inc.)

Sample WLAN Project Plan			
Step	**Plan and Communicate**	# of Days	Running Total Time in Days
1.00	Determine the scope including the number of schools, size of the required coverage area(s), number of users to be supported	2	2
1.01	Set goals and expectations	0	2
1.02	Define roles of project team members	1	3
1.03	Define budget	1	4
1.04	Draft mid- to long-term plans (1 to 5 years) to allow for scalability in line with strategic business planning	1	5
1.05	Decide on wireless encryption and authentication protocol	1	6
1.06	Determine minimum security requirements	1	7
1.07	Identify compatibility and/or required upgrades and configuration changes to existing hardware, software, network architecture and maintenance/support structure (e.g. Authentication server, Internet connectivity, backbone switching architecture, NICs, VLAN supporting firewalls, etc.)	4	11
1.08	Outline usage and applications to be run on the WLAN to estimate additional bandwidth, speed and latency requirements	2	13
1.09	Select target client:AP ratio, approximate cost per AP and percentage of AP to total budget (e.g. 10:1, $250 and 20%)	0	13
1.10	Determine user policies for the wireless network	1	14
	Sub-Total	14	14
	Site Survey		
2.00	Obtain floor plans for all implementation sites	3	17
2.01	Determine how many APs it will take to provide a signal to the desired coverage area	1	18
2.02	Physical AP placement map	1	19
2.03	Identify signal trouble areas and physical construction or environmental challenges	0	19
2.04	Diagram channel layout of APs	1	20
2.05	Confirm hardware compatibility (include desired legacy hardware, new hardware and current or future for student owned device standards)	2	22
2.06	Verify that each APs location is physically secure	0	22
2.07	Verify that there is a power source near the intended location for each AP or PoE compatibility	1	23
2.08	Confirm there is a way to run a patch cable between your wired network and each AP and/or APs to be used as repeaters.	1	24

2.09	List specialized antennae requirements	0	24
2.10	Determine AP network cabling distances and are within CAT-5 or 6 limits (~100m)	1	25
	Sub-Total	11	25
	Procure Hardware, Software, Services and Training		
3.00	Research and review vendor WLAN solutions	3	28
3.01	Meet top two to three WLAN vendors for face-to-face presentations on their solutions	5	33
3.02	Purchase infrastructure upgrades identified in planning stage (e.g. District head office and/or school site WAN speed increase from 10Mb/s to 60Mb/s and switch upgrades from 100Mb/s to 1Gbps)	21	54
3.03	Buy the necessary AP, controllers, management software, and wireless NICs	5	59
3.04	Record the MAC address of all hardware	1	
3.05	Purchase other upgrades identified in planning stage	5	64
3.06	Record and distribute all vendor and out-sourced service company or VAR technical support contact information to implementation team	1	65
3.07	Register with all vendors using a centralized and common email address for alerts, support notifications, etc. (e.g. WLAN@yourdomain.com which is aliased to all relevant members)	1	66
	Sub-Total	42	66
	WLAN Implementation and Security		
4.00	Configure and install WLAN controller	1	67
4.01	Install a pilot set of APs at one location	1	68
4.02	Configure clients	1	69
4.03	Test and fine tune client:AP ratio	1	70
4.04	Adjust AP and antennae placement	1	71
4.05	Roll-out all APs at all locations	3	74
4.06	Record physical location of all hardware (by MAC addresses), use floor plans	1	75
4.07	Configure remaining clients	1	76
4.08	Test and fine tune	**3**	79
4.09	Configure and implement security settings for VPN, VLAN, NAC and/or other hardware and software (advised to perform on pilot area, test, then roll-out)	**5**	84
4.10	Vendor product training on Controller management software. Reset all passwords to high level of entropy, get familiar with interface, features, capabilities and reports	**3**	87
	Sub-Total	**21**	87
	Assess project and repeat above steps as necessary	**10**	**97**
	Integrate WLAN into IT strategy and maintenance and support structure	**10**	**107**

Scope

Ultimately, the scope is defined by budget.

{ 10 x 10 } ≠ 100

Ten schools with 10 APs each is not the same scope as one school with 100 APs

A common pitfall with implementation of wireless solutions is missing the hard costs associated with a total solution. For example, simply spending 100% of the budget on mobile devices would not be a solution. In the same light, allocating the entire budget for just APs and laptops still is not a viable solution.

So what are the inter-related elements to be considered to find the optimal balance and achieve maximum coverage and quality of experience for the wireless users, students and staff? The following matrix will assist with identifying 25 key elements that are all factors to be considered in a WLAN implementation in a K-12 school district. There are many more, however, and filling in these 25 will direct the appropriate resources, timelines, policies and solutions into place.

Table 7 - WLAN Scope Elements (Network Integrators of Canada Inc.)

APs: Thin or Thick	Existing Internet Pipe at School Site	Traffic Topology	Desktop Management	Time
Controllers	Existing Internet Pipe at District Head Office	Client:AP Ratio	Compliance (NAC)	# of School Sites
# of Laptops	Security Tolerance	IT Staff	Standardized vs. Non-Standardized Clients	Budget
# of Student WLAN Users	Existing Network Hardware	Out-Sourced IT Service Partner	Scalability	Usage Policy
Application Types	Coverage Area	WLAN Vendor	Life Cycle	Ongoing Support Requirements

Client-to-AP Ratio

Many different factors impact the performance of your WLAN such as:

Internal Factors:
- The shared nature of the communication medium;
- The access mechanism for the medium;
- The use of a limited number of communications channels; and
- The available bandwidth.

External Factors:
- The number of users;
- The types of devices communicating across the WLAN;
- The types of applications used on the network; and
- The degree of mobility that is demanded by the user community.

Knowing the traffic types and usage patterns on the WLAN is fundamental to designing a solution that not only performs correctly, but also delivers a relatively consistent level of service. As such, providing the WLAN with the proper number of APs is a contributing factor to creating a WLAN that meets a performance baseline. The simple translation is that determining and managing the number of simultaneous connections will be critical to controlling a WLAN environment.

The industry has converged on the metric "client-to-access point ratio" to denote the number of users a single access point can consistently support. However, do not take the term client at face value. Indeed, a student that uses the WLAN primarily for e-mail and web browsing will have different bandwidth requirements than a student using Computer Aided Design (CAD) programs using the WLAN mainly for streaming intensive applications. As such, carefully consider the types of clients and their respective network needs, such as bandwidth and throughput requirements.

Do not make the assumption that more senior students will be utilizing more intensive applications either. Primary students' applications may likely be more graphical or interactive, and high school students may well be utilizing simple file access for documents and less intensive applications.

The client-to-AP ratio is expressed as a number such as 10:1, and not more than 15:1. In this case, the number 10 or 15 represents the recommended maximum number of clients that can be associated to an AP at any given time.

Exceeding this ratio will degrade the expected performance. Three different strategies can be used to determine what an environment's optimal client-to-AP ratio is. Benchmark tests to identify exactly what works, classify users and traffic types to generate more granular client-to-AP ratio specifications, or simply adopt client-to-AP ratio guidelines that have been published by most vendors. Each strategy has its merits and drawbacks.

Benchmarking enables the most precise identification of the client-to-AP ratio. Local variations are measured and the ratio can be optimized depending on the exact user profiles and needs. However, not only is this approach time and resource intensive, but it also creates a dated snapshot. If the environment changes, for example, and adjacent classes running simultaneously introduce new software with different traffic signatures, the benchmarks will no longer be accurate.

By classifying both traffic and users, some degree of customization can be captured. The process is relatively straightforward and can be performed by your network architects and designers. A challenge likely faced with this method is the identification of the correct segmentation of the users and traffic types. Do not reinvent the wheel. Follow the classification guidelines as set forth in the architecture. Given the benefits of more accurately identifying a client-to-AP ratio that yields a more consistent and satisfactory WLAN user experience, this approach is recommended.

The final strategy is to accept the recommended client-to-AP ratio as published by the WLAN equipment vendor. Even though this is the easiest solution, there is potential for over- or under-provisioning the number of APs because the information provided by the vendor does not consider the specific user-base requirements. However, use the WLAN vendor's published recommendations as a rough guideline.

3.4 Technical Deployment Considerations

Network

Compatibility Overview

Some key points to be considered are:

- Wireless access and authentication is hardware specific;
- Older wireless cards will not support WPA2. Computer upgrades may be required to meet security policies;
- If using thick APs, use all the same brand and model for ease of configuration and management; and
- Configuration files can be pushed out to clients if they are standardized.

A factor that affects scalability is compatibility, and this is a two-pronged consideration – compatibility of wireless technologies with one another and compatibility with wireless devices, especially the network adapters built into many of today's laptop computers. A big advantage of 802.11g over 802.11a is its backward compatibility with 802.11b. This means that starting small with an inexpensive 802.11b AP and then later replacing it with an AP that supports both b and g. Computers that have 802.11b network adapters will still work, but at the lower 802.11b speeds. Replacing NICs gradually makes for a smooth transition. Switching to 802.11a, everything will have to be replaced immediately because it is not backwardly compatible with old 802.11b equipment. Current clients embedded in laptops and tablets typically support 802.11n and both frequency bands. Investigation is still required because a vendor may indicate his product supports 802.11n, but it does not support both frequency bands. These new clients are still backwards compatible with older 802.11a/b/g technology providing the radio in the client has both frequencies. The AP will use the lowest common speed denominator that is allowed by its configuration. All broadcast traffic from the AP will be sent at the lowest common data rate allowed. If there is a single 802.11b client in the coverage area, and the AP is configured to allow it, then the broadcast traffic and beacons will be sent at 1.0 Mb/s, severely limiting even an 802.11n capable AP.

So frequency of operation is as important as the technology or standard that the client can support.

Architecture

Things to consider when determining network architecture include:

- Backbone inter-connect speeds at individual school sites and/or (if hub and spoke design) at district head office site, may need upgrading to support new users;
- Upgrading to 802.11n APs requires Gigabit switch ports to handle the traffic that the AP is capable of;
- VLANs: is there capacity for more to segment the WLAN;
- Firewall policies and restrictions: e.g. block the AP to WLAN controller traffic; and
- VPN capacity. Checking actual VPN throughput is recommended.

Security

Wireless networking can become a massive security challenge if not setup and managed appropriately. As such, it is important to have an effective wireless networking policy in place across the school authority's network.

A big security challenge with wireless networks is that they transmit potentially sensitive information over the airwaves. This means that the information flowing across the network can be intercepted by anyone within range who has a laptop equipped with a wireless network card. Likewise, wireless access points provide a way for hackers to enter networks without having to deal with the constraints normally associated with an Internet based attack. As such, wireless networks can pose a huge threat to network security unless there is a good wireless network security policy in place coupled with the latest security technology (e.g. WPA2 with EAP, see Chapter 4 on Security).

Matching Wireless Policy to the Administration Model

The administrative policy should be a document that specifies how wireless hardware will be connected to the wired network, and by what type of user. This is critical because, as with many school authorities, the IT department is decentralized with technicians working at various locations including their home, school sites and at central office. Be sure to select one standard encryption methodology for all schools. Employ a top-down approach and ensure this decision is implemented at all school sites.

Develop a strong and encompassing wireless networking policy. One clause strongly recommended is that wireless APs must only be attached to a dedicated network segment, and not to a segment containing other network resources.

Hardware

Points to consider include:

- May require switch upgrades to support PoE, VLANs or Gigabit capacity to support 802.11n APs;
- Older hardware is incompatible with new security standards; and
- Can older hardware support the new wireless cards? Is there room for them?

Software

Application characteristics must be analyzed if this traffic is to flow over the WLAN. It is essential to outline this in the policy to protect and ensure scalability as planned.

Performance is not limited to the throughput that a client can achieve. It is also directly related to the client keeping its network connection and communication session intact. When roaming from one AP to another, there is a small amount of time during either authentication or association during which the client will effectively be without a link. The duration of the lost link will determine if and how applications will be impacted. For data centric session roaming, this link loss is almost unnoticeable to end users. For time sensitive media session roaming, such as VoIP over the WLAN, this can require additional network optimization.

Applications exhibit a distinctive sensitivity to the duration of a lost link. Transactional applications such as e-mail and web browsing are relatively insensitive, whereas real-time applications such as voice and video are highly sensitive. Ensure that fast roaming is enabled to make authentication occur promptly enough to not affect the core WLAN application suite.

Application bandwidth requirements can be analyzed by the software vendor's specification or manuals. A common issue with networked applications is that they are developed with little or no consideration for the resources they require from the communications infrastructure. Application developers take into consideration the notion of the network, but typically fail to consider bandwidth and latency implications. The false assumption is that the network is always available, that bandwidth is unlimited and that congestion and delays do not occur. As such, even though the applications and the network are tightly coupled, they are typically developed and deployed as independent components. It is exactly this decoupling that creates the burden of carefully planning a WLAN for successful support of the extension of applications to the wireless environment. Hence, start with the premise that the average application is not aware of the transport medium it is using. They treat both wired and wireless networks identically.

The challenge of applications not being aware the network is compounded with WLANs. Indeed, most applications are developed for wired environments. Specific characteristics of WLANs are their lower throughput and higher latency than their wired equivalents. This is typically not a problem for the bursty applications. However, WLANs can cause additional challenges for applications that demand high data rates or deterministic behaviour. The interaction between applications and the network is only one of the challenges that must be tackled when defining WLAN architecture. Defining a wireless architecture to support voice and video also introduces specific problems that must be considered. The considerations include provisioning sufficient bandwidth for latency-sensitive applications, implementing a quality of service (QoS) solution, and ensuring fast-roaming capabilities between cells.

Speed requirements

Speed and distance can be important factors in the scalability of a WLAN. As schools integrate more and more technology into learning and teaching, policy changes such as students bringing their own devices onto WLANs will add more and more users. In addition, more bandwidth will be required for the transfer of larger files and for higher bandwidth technologies such as streaming audio/video, real-time conferencing and so on

802.11a and 802.11g provide more scalability in this regard than 802.11b and 802.11a. Distance range can also be a factor in the scalability. Should a school site expand physically, more APs to reach the areas with 802.11a would be required than with 802.11b or g.

802.11n is beginning to solve some of these issues and make wireless to the user a relatively painless and seamless activity.

Ensuring that all of your solution is compatible with 802.11n will provide scalability to higher speeds down the road.

Site Survey

A site survey identifies the optimum locations for APs, given the access and bandwidth requirements outlined by the plan and design. It is important to note that a quality site survey is much more than a simple physical walk-through of a school. An experienced network technician will use a combination of specialized electronic tools, practical experience and specific floor plans showing the locations of one-to-one learning environments. An effective site survey should indicate how many devices should be able to use the intended applications concurrently, and at what locations within a school building or buildings they can support. The original form of site survey was a combination of physical and trial and error. An AP can be placed in a possible location and tested for coverage, then added another and so on. Now automated, site survey tools exist to provide an initial plan for AP locations. These tools import floor plans from CAD files or jpeg files and allow users to overlay the APs in the software and generate a heat or coverage map to see if the coverage and capacity meets the system requirements. Most controller base wireless vendors have a system planning utility that can assist in this process. If a vendor has been selected, use their automated sites survey utility. Aruba has RF Plan, Cisco has the Cisco Configuration Assistant and Ruckus Wireless has the Zone planner to name a few. In some cases these utilities are a free download from the company's website.

When the survey is done, a report should be developed which includes:

1. A summary statement on how the WLAN is to be used and what it is intended to achieve, including the audiences and applications. Ideally, at least a three-year road map would be useful.

2. An analysis of the physical structure and its fitness for wireless resources.
3. Reports of the data resulting from the tools for predicting the likelihood of success of a wireless implementation and the optimum placement of APs. These tools can predict possible problems with high demand, coverage conflicts and overlaps and dead spots. This should include the number of APs needed.
4. Because the rule of thumb is a maximum of 10 to 15 simultaneous users per AP (e.g. using 802.11b), the report should predict the current ratio of users to APs.
5. A map of the preferred placement of APs based on the site survey. This should also include information on the anticipated configuration of each AP for use in management and security of the WLAN environment including 802.11 a, b, or g channel selections. Some of the more obvious configuration items are the name and channel of the AP, the coverage area, authentication and encryption type, IP addresses and MAC addresses (to be entered upon procurement of hardware).
6. Identify neighbouring APs and WLANs.
7. List desired coverage area(s). Identify any odd-shaped buildings, corridors, aisles, and similar limitations that might affect the placement and/or number of APs and antennae. Through proper selection and placement of antennae, coverage can be extended into desired areas, overcoming physical obstacles and multipath interference.
8. Signal characteristics throughout the coverage area including strength, signal-to-noise ratio (SNR) and *packet retry count* (the number of times packets were retransmitted for successful reception).

The magic number for packet retry count is 10 percent. There should be no more than 10 percent in any area. Use packet retry in tandem with the SNR reading for a good picture of signal quality. The signal might be strong enough, but because of noise or multipath interference, packets are re-sent. Without an SNR reading, you cannot tell if packet retries spike because you are out of range, there is too much noise or the signal is too low.

For further information on this and a sample list of vendors, see Appendix B and D.

AP Location for Site Survey

When performing a site survey, situate the APs as close to their final mounting positions as possible. This helps resolve any problems that might creep up after mounting the AP. In most cases, APs should be mounted at ceiling height. In areas with high ceilings, take advantage and mount them between 15 and 25 feet as this will help to account for large influxes of physical student body traffic. If mounted at this height, power delivered to the devices must be addressed. PoE is optimal to avoid time and cost associated with electrical outlet installation, and can also save a lot of headache and expense.

Physical Security

Although vandalism has not been identified as an issue in any of the districts interviewed, it might be desirable to keep the AP out of sight and reach in less frequently monitored areas. If the AP is placed above ceiling panels, antennae should still be placed below the panels for optimal reception. If this is the case, purchase an AP that fits for remote antenna capability and do not put the antennae unnecessarily far away from the AP as there will be increasing signal loss.

Check your local building and fire codes. You might need plenum-rated APs and cabling if they are placed above the ceiling tiles in open air return systems.

Signal Strength

In general, objects absorb or reflect signal strength and degrade or block the signal. Identify any potential obstacles or impediments in the area to be served. Examples of common objects that a school's WLAN may encounter are:

Walls – especially if the wall is composed of heavier construction materials, such as concrete. Also note any physical construction firewalls in the area.

Ceiling tiles – particularly if they are made of material such as metal.

Student Body – For example when the bell rings and a wave of bodies flood the corridors, a dramatic loss of signal can occur during these times.

Furniture – especially pieces that are primarily made of metal.

Natural elements – such as water, trees, and bushes – not only outdoors, but also in many courtyards or other interior public spaces.

Wood floors – can allow floor-to-floor interaction between APs causing channel interference or other noise. Think three dimensionally.

Classroom doors – these should be closed before beginning the survey. This shows how the WLAN performs in real, day-to-day functioning, so that is how it should be surveyed.

Coated glass – transparent glass generally does not greatly degrade signal strength. But it may do so if it is coated with a metallic film or has a wire mesh embedded in it.

Cell Layout and Channel Usage

Most scenarios require more than two APs to cover the appropriate area within a school. Therefore, consider the layout and configuration of more and more APs to scale the design to fit the wireless environment.

For example, to cover the entire area of a wing of a school or one floor of the entire building, APs must be placed at regular intervals throughout that space. Information from the site survey is vital in deciding on final AP placement, as actual live measurements can be used with an AP staged at various points in the actual space.

The two basic elements of designing a WLAN are:

- Sizing the AP cells; and
- Selecting channels for the AP cells.

Sizing AP Cells

The size of AP cells determines the number of APs that must be purchased and deployed to cover an area. However, the design should not be driven by cost alone. AP cell size can also affect the performance of the APs as clients move around or gather in one place. Within a single AP cell, all the clients associated with that AP must share the bandwidth and contend for access. If the cell is large, a large number of clients could potentially gather and use that AP. If the cell size is reduced, the number of simultaneous clients can also be reduced thus offering higher throughput potential.

Large cells can allow clients to step their data rates down as they move farther away from the APs. For example, when an 802.11b client is near an AP, it can use the highest data rate (11 Mb/s). As the client moves out away from the AP, the data rate can be reduced to 5.5, 2, and finally 1 Mb/s. Clients may need to use only the highest data rates in a cell, which can be accomplished by reducing the cell size.

Generally, the AP cell size is driven by the APs transmit power. Higher power equates to greater range, so the power must be adjusted so that the APs signal does not propagate into nearby AP cells operating on the same channel, which should be dramatically minimized with an efficient layout plan. The controller based system can adjust the power dynamically of all the AP's under its control to minimize interference. Once the AP cells have been sized and pinpointed, clients should be able to associate and roam at any location within the coverage area.

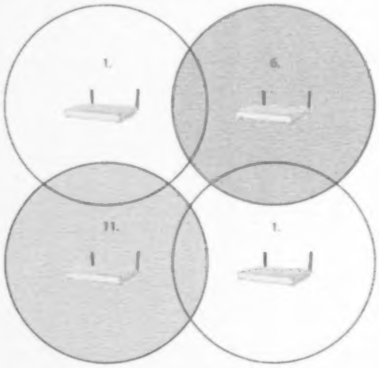
Throughput and bandwidth are not created equal. Due to the fact that the client and the AP are half duplex devices, the bandwidth of the channel must be divided in half, then take into account overhead, Management Frames and any other traffic that is not part of the data transfer to determine actual throughput of a transmission at a specific range. The highest bandwidth for 802.11a is 54Mb/s and typical throughputs are in the 22Mb/s range.

As a very loose guideline, consider the maximum peak throughput of a wireless cell divided by the number of simultaneous clients to determine a maximum data rate per user. Factoring in the overhead of 802.11 encapsulation and bandwidth contention, 802.11b can offer around 5 Mb/s through each AP, whereas 802.11g and 802.11a offer up to 22 Mb/s. This means, for example, in an 802.11b cell with 25 clients, each client would have a maximum throughput of 5 Mb/s / 25, or 200 Kbps. In an 802.11a or 802.11g cell, those same 25 users would have 22 Mb/s / 25, or about 1 Mb/s. An 802.11n AP radio with at least 2 radio chains, the Guard Interval set to the shortest value of 400ns and utilizing a 40 MHz channel (which indicates a 5.8GHz deployment) can provide a bandwidth of 300 Mbs. When 802.11n is deployed in the 2.4 GHz spectrum, in order to still have 3 non-overlapping channels, it uses the longer guard interval of 800ns. At these setting the maximum bandwidth is 130 Mb/s. Once again at the very highest the throughput is close to ½ the bandwidth. Once can achieve 150 Mbs for an ideal deployment in the 5.8 GHz and 65 Mbs in the 2.4 GHz spectrum.

WLAN Channel Layout

To minimize channel overlap and interference, AP cells should be designed so that adjacent APs use different channels. 802.11b and 802.11g limit using channels 1, 6, and 11. The cells could be laid out in a regular, alternating pattern, as the following Figure 18 illustrates.

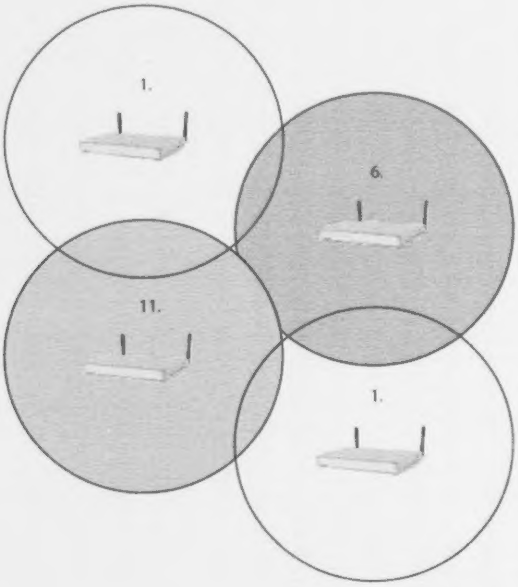
Figure 16 – Alternating Channels (Network Integrators of Canada Inc.)



However, in the very center where the cells meet, there is a small hole in RF coverage. This may not be a significant problem depending on the required layout of coverage area, however any hole can pose a problem if a client roams through the area, his wireless signal will probably drop completely. As well, it cannot be solved properly even if the cells were brought closer together to close this hole, as the two cells using channel 1 would overlap and begin interfering with each other.

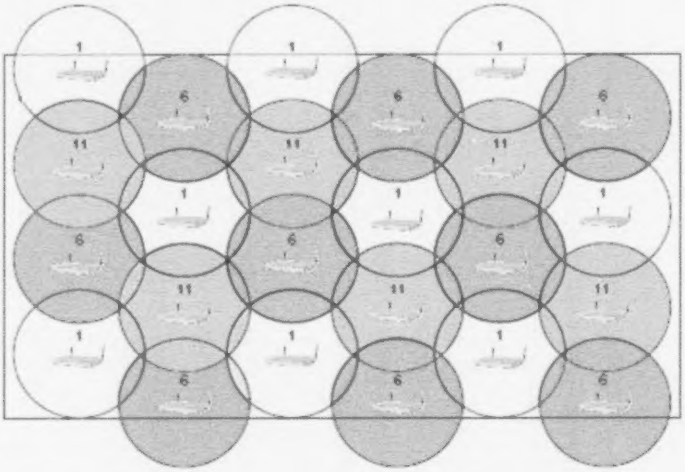
The solution is to lay out the cells in a honeycomb fashion as illustrated below. The honeycomb pattern is seamless, with no holes. As well, the cells using the same channels are well separated, providing isolation from interference and unlimited scalability in design. As far as ordering channels in the pattern, several different variations are available using combinations of the three channels.

Figure 17 - Alternating Channel Pattern (Network Integrators of Canada Inc.)



Notice that as the client shown in the channel 1 cell moves around, it will roam into adjacent cells and change channels. In order for roaming to work as it is intended, a client must be able to move from one channel into a completely different channel. Alternating channels is referred to as channel reuse. The basic pattern shown in the previous figure can be continually repeated to expand over the required coverage area, as the next figure illustrates.

Figure 18 – Channel Reuse (Network Integrators of Canada Inc.)



These examples have been illustrated with 802.11b/g setups. It is even simpler with 802.11a due to the larger number of channels available for use. However, the design is quite different. 802.11a can utilize four, eight, or even twelve non-overlapping channels, so chances of adjacent cells using the same channel is much lower.

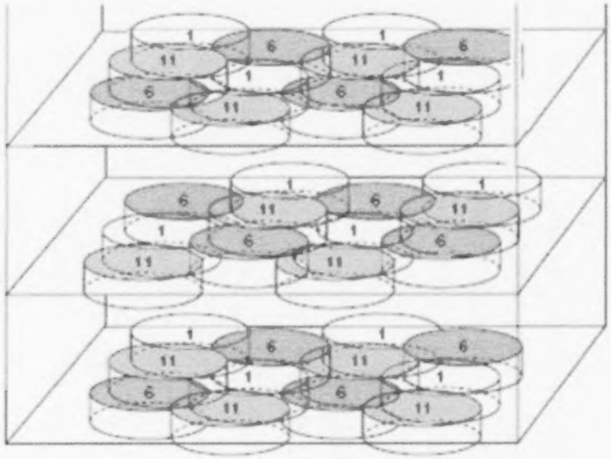
So far, only two-dimensional scenarios have been assessed, but should more than one floor be included in the coverage area, a three-dimensional design must be implemented.

Recall that an RF signal propagating from an antenna takes on a three-dimensional shape. As outlined in the antennae section, an omni-directional antenna's coverage pattern is donut shaped (with the antenna being in the middle) compared to unidirectional which appear as more cone shaped in the direction the antenna is pointing.

The following example uses omni-directional antennae. The antenna signal extends outward, giving the cell a circular shape above and below on the floor and ceiling, possibly affecting AP cells on adjacent floors.

Cell channels on adjacent floors should be staggered both beside and between floors as presented below.

Figure 19 – Channel Reuse Across Multiple Floors (Network Integrators of Canada Inc.)



Alternate channels adjacent to one another on the same floor, and between floors for a non-overlapping design. Channel 1 on the second floor should not overlap with channel 1 directly above it on the third floor or below it on the first. The cell size, AP power, and channel assignment all have to be coordinated on each and every AP. Roaming also becomes challenging if clients are permitted to roam across the school's wireless network.

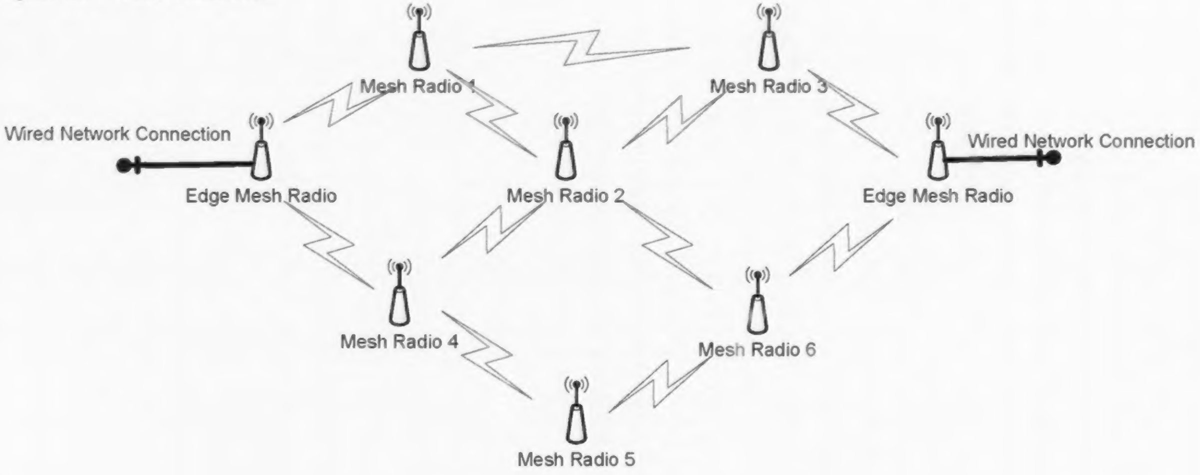
Point-to-Point Bridging

The wireless bridge link functionality is not covered in the 802.11 standard. This means that wireless vendors who have this functionality in their devices may use proprietary protocols for the bridge devices to communicate. Therefore, to enable this function, devices from different vendors would not interoperate. Bridging takes place where it is not feasible to run a network cable between two buildings to join their respective LANs into a single Layer 3 broadcast domain or due to budget limitations whereby wireless repeaters are cheaper than a hard wired solution. If the two buildings are a reasonable distance apart and ideally in direct line of sight with each other, wireless bridges can be configured. In this mode, wireless APs are configured to forward traffic between each other and not act as wireless APs for client access. The most typical scenario for this is to use dual AP radios, with the 5.8 GHz 802.11a or n radio for the bridge link and use the 2.4 GHz 802.11g or n radio for access at the bridge link locations as well. Some APs can be configured to provide bridge capabilities with wireless clients as well.

Mesh Networking

Mesh wireless networks have been available for the last 6 years or so and are most typically used to cover high density outdoor areas. These devices are used in areas where there is no wired infrastructure to connect the APs. Their primary features are their capability to withstand the outdoor environment and that their "a" radio is typically used for a backhaul. As opposed to a bridging solution the mesh or "a" radio can communicate with any other mesh radio within range and utilize the best route that will take network bound traffic on. The "g' radio provides the drop or connection to the wireless clients that may be in the coverage area. One hurdle that currently exists is that there is no approved standard for wireless mesh and the mesh protocols in use are proprietary. In the drawing, a mesh radio responsible for connecting local traffic on its "g" radio can use the best route back to the wired network connection. Each mesh radio has multiple routes to the wired network and should a specific route fail for any reason it will recalculate and switch routes.

Figure 20 – Mesh Networks



Noise and Interference

Noise from cordless phones, wireless headsets, Bluetooth devices and other non-protocol devices can interfere with an AP trying to send or receive data. The site survey should identify sources of signal noise present in each deployment area so that the WLAN can avoid at least the already existing noise sources, or remove the sources of noise.

Consider the following four common misconceptions surrounding noise and interference for WLANs:

Misconception 1: "WLAN hardware addresses interference automatically."

Most centrally coordinated wireless controllers, or smart switches, do manage RF interference problems, however, they are limited. In response to detection, they can try to change the 802.11 channel of the APs in the area of the interference and they also can manage the power settings of individual APs to create a balanced roaming boundary an limit interference from its own APs

Some devices (Bluetooth or cordless phones) that cause noise actually change frequencies regularly, so it is impossible to change channels away from them. They consume the entire band at different points in time. It is critical to be able to identify the actual source of interference. Identify what the device is and where it is located in order to determine the best course of action to handle the interference. This may be removing or relocating the device. Another solution may be to shield the device from impacting the network.

Misconception 2: "RF sweeps in the site survey stage find all sources of interference."

One of the biggest challenges about interference is its intermittency. The interference may occur only at certain times of day (e.g. when someone is operating the device like a Bluetooth headset), or on certain days of the week. It is very easy for someone to introduce one of the many devices that operate in the unlicensed band into the environment at any time and thus it is a constantly moving target.

Misconception 3: "The WLAN network is working fine. There is no interference."

The 802.11 protocol is designed to be resilient to interference. When an 802.11 device senses interference, it will merely wait to transmit until the interference burst is finished. If the interference burst starts in the middle of an ongoing 802.11 transmission (and results in the packet not being received properly) then the lack of an acknowledgement packet will cause the transmitter to resend the packet. Packets get through, however increasing the PRC above 10% makes for an inefficient WLAN design.

The result of this waiting and retransmissions is that the throughput and capacity of the WLAN are significantly impacted.

Misconception 4: "A high density of APs solves interference issues."

The inexpensive nature of (especially thin) 802.11 APs makes it tempting to deploy them higher density than actually required, such as in every classroom. This type of deployment has the benefit of greatly increasing the capacity of the network.

Unfortunately, when deploying a dense network of APs, it is necessary to reduce the transmit signal power of each. If the power is not reduced enough, the APs generate interference with each other, known as co-channel interference. The reduction in the transmit power of the AP offsets the potential benefit of interference immunity. Therefore, the interference resistance of a network with a dense deployment of APs is not significantly better than that of a less dense deployment.

Distance

How far can you go?

The table below shows typical ranges that can be expected from an 802.11a/g WLAN design.

The reason for slower speeds is that material objects absorb the radiation. The amount of absorption varies with the material, but generally the more mass in the object, the more the absorption. Metal provides copious amounts of shielding due to how it interacts with electromagnetic fields. Furthermore, the angle that the signal passes through the wall affects the amount of interference.

Table 8 - 802.11a/g Speed and Range (Network Integrators of Canada Inc.)

Speed*		Range*	
Throughput Speeds (maximum)	**Effective Throughput Speeds* (typical)**	**Indoor**	**Outdoor**
2.5	1	100 m	500 m
5.5	2.5	75 m	250 m
11	5.5	50 m	100 m
54	23	25 m	50 m

*Speed and Range defined here can be used as guidelines only and have been determined based on generally accepted industry information coupled with hands-on experience of WLAN implementations.

Figure 21 – Throughput of 802.11n is 7 times faster than 802.11g

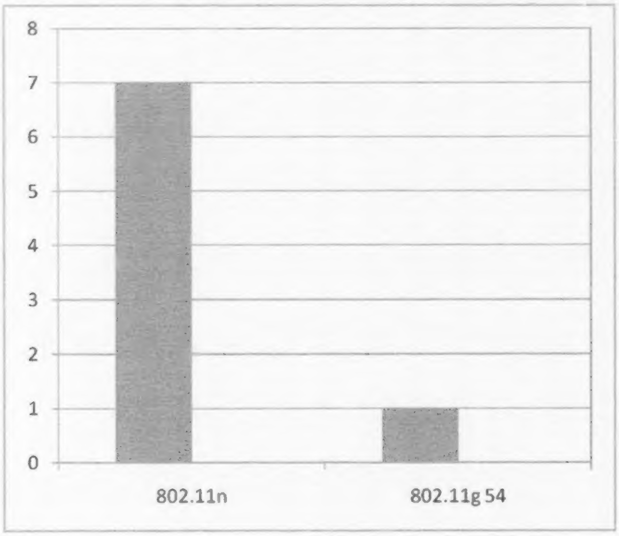


Figure 22 - At 300 feet 802.11n can transmit up to 70 Mb/s whereas 802.11g can only be transmitting at 1 Mb/s

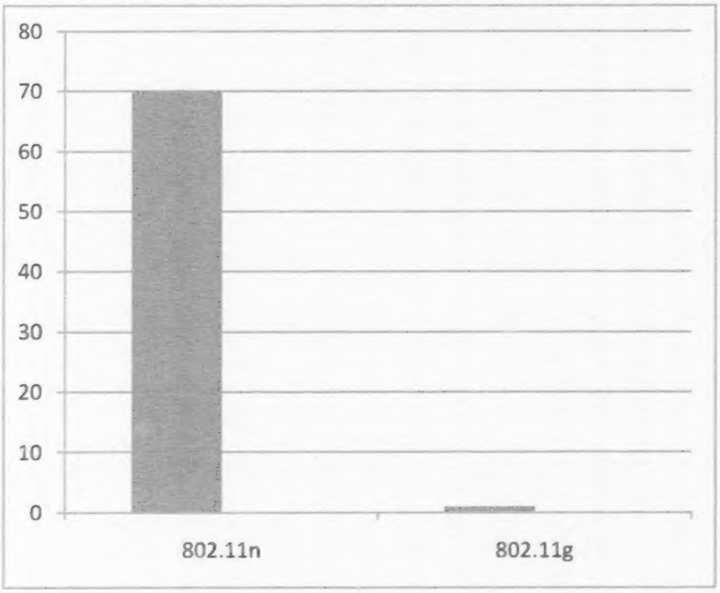
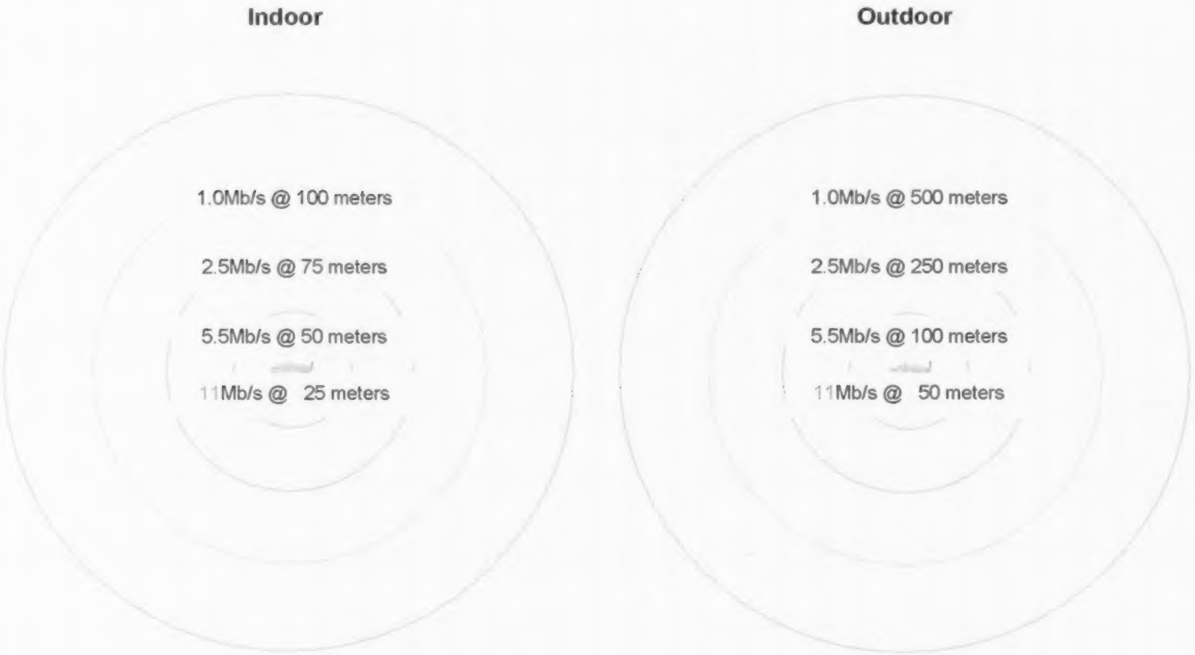


Figure 23 illustrates the same for an 802.11b WLAN with a maximum speed of 11Mb/s.

Figure 23 - Indoor and Outdoor Speed and Range (Network Integrators of Canada Inc.)



Electrical Requirements and PoE

The simplest answer here is Power over Ethernet (PoE). This should be utilized for all APs, otherwise the placement of APs must be within reach of a standard power outlet. There are four options to power APs. The options depend on whether or not the AP receives power from a power supply or if it receives inline power. It was originally standardized as 803.3af, It is now included in the 802.11 standard since the 2005 release. Unfortunately that standard does not provide the power required for an 802.11n AP. So the 802.3at standard was ratified in 2009 often referred to as PoE+ and embedded in the latest 802.11n 2009 standard. This provides the additional power (30Watts) for 802.11n APs as well as defines the used of PoE over 1000 Base-T wiring.

This new standard allows backwards compatibility to power 802.3af compliant devices as well. The original 802.3af standard was fairly easy to describe. It used a single pair of wires and at the 100m Ethernet cable maximum could provide 12.95 watts with a source voltage of 48 volts. The new 802.3at standard can use all four pair of wires and with a source voltage of 56 volts can provide up to 60 watts of power at the 100m maximum Ethernet cable length. As well the Power Sourcing Equipment (PSE) needs to be addressed as well. Comparing two switches from the same vendor with 24 PoE ports, one 802,3af and the other 802.3at, the 802.3at capable switch will require up to an additional 10 Amps from the 110V service that powers it. It is not cost effective to upgrade all switching hardware to Gigabit 802.3at capability immediately. A planned migration should be implemented. The different power options for an AP are listed below. The four connection options are:

- A switch with inline PoE;
- A patch panel with PoE;
- A power injector between the switch and the AP; and
- A local power supply (i.e. an electrical outlet near the AP).

Table 9 PoE Comparison

Standard	Voltage	Source Power	Load Power
802.3af PoE	48 VDC	19.2 Watts	12.95 Watts
802.3at PoE Plus	56 VDC	72 Watts	60 Watts

If you use the APs 5-GHz radio, make sure your switch and patch panel provide enough power to the device. The 2.4-GHz radios are widely covered, but there might not be enough support for the 5-GHz radio.

Cabling Requirements

Points for consideration include:

- Each AP requires connectivity to a switch on the network. This often means more cabling runs must be pulled;
- Future-proof any cable that has to be installed. Use the higher rated cable to allow for future requirements. Using CAT6 instead of CAT5e, for example, ensures higher data rates reliably when required.

You must also consider the distance between the AP and the switch. The maximum range for 100BaseT Ethernet is 100 metres.

Physical Construction Elements

Building structure can be a significant source of interference. Most schools are constructed with concrete, brick and sheet rock. While materials, particularly concrete, will interfere with WLAN signals, sheetrock only blocks a small portion of a signal, making it WLAN-friendly. However, when deploying WLAN into older buildings, problems dramatically increase and may require the deployment of more APs than initially planned on paper. A detailed site survey of buildings will best answer this question. Older schools with wooden walls that were reinforced with a chicken wire-like material can cause significant interference and dead zones. Even though the material is not extremely thick, its shape and location throughout the walls and sometimes in the ceiling of a room effectively blocks, or at least disrupts, a WLAN's Wi-Fi signal.

Additionally, rebar-reinforced concrete can sometimes create a similar problem. This problem could be considered either a pro or a con. It can provide a way to secure the WLAN to concentrated areas and not have leakage of coverage outside of the building.

Both the type of material in an obstruction and the angle at which antennae point through obstructions affects signal degradation. Obstruction materials include plasterboard walls, cinder-block walls, concrete walls, glass with metal frames, metal doors in brick walls and steel-mesh reinforced walls. The greater the angle at which the antennae directs through an obstruction, the greater the signal loss will be.

A generic rule of thumb is that the signal is one-fourth as strong when twice as far away, *barring* any additional obstructions.

Security Considerations

The inherently open nature of wireless access, compared to the wired world, creates significant security concerns, chief among them, user authentication, rights enforcement and data encryption. Without the minimum recommended level of security as defined in Section 2.2 Wireless Security Standards, broadcast signals often travel into public areas that can be accessed by individuals who have not passed through any type of authentication process to validate their presence onto the WLAN.

The security solution must provide Network Access Control in different ways for different types of users who may require connecting at the same school, such as a teacher, student or visitor. Some users, such as staff or principals, may be entitled to total or broad access to all school and/or district resources. Other users, such as guests or students, may be entitled only to more limited access, like filtered Internet browsing.

The site survey should note where guests, contractors, or other non–staff users may be located, so that appropriate security solutions can be created for those areas.

Robust passwords form the foundation of security.
They should be sufficiently strong to prevent easy guessing or hacking. Use both UPPERCASE and lowercase alphanumeric characters in addition to special characters. Use no less than a 10 character password. An example of a robust password is abc123XYZ!@#.

Impact of Device Standards, Ownership and Mobility

It is essential to understand the difference between non-standardized and standardized client devices, laptops that stay at school only versus ones that students take home, and one versus many device types to be supported by the district (e.g. iPhone, iPad, laptop, and BlackBerry). This section shows best practices surrounding security, optimal maintenance, support and management under the following scenarios:

School-owned: Standardized on Single Device Type (e.g. Laptop)

- This is certainly the easiest method to manage and support.
- All hardware is the same, each user group will have an image of the system that can be deployed for new users and correcting errors on old systems that are unstable.
- Support costs and mean time to repair will go down.
- Can have spare laptops ready for deployment.
- Can dictate access levels on the system itself and exhibit great control of the system environment to increase security and lower support costs.
- All laptops are the same regardless of user needs. Go with a balance of price and performance.

School-Owned: Multiple Device Types (e.g. Laptop1, Laptop2, PDA1)

- Can have spare laptops ready for deployment or swapping, however the more models/types to be supported strains budgets and support requirements (e.g. training).
- Can dictate access levels on the system itself and exhibit great control of the system environment to increase security and lower support costs.
- Allows for greater flexibility for user needs. Graphic users can have higher powered laptops whereby users that only use word processing can be given less powerful and lower cost laptops. There can be a tremendous cost savings here.
- Can still have spare laptops on hand for support and deployment.

Integration of Personally-Owned Devices

Personally-owned devices are student or staff-owned technologies that are brought into schools. Schools in Alberta have been exploring the use of personally-owned devices for almost five years. In addition to the increased flexibility it can offer to students, it is also seen as a more fiscally sustainable way of expanding the use of laptops and other devices to all students.

Alberta Education is producing a Personally Owned Devices guide to support administrators and policymakers' decisions making process around planning, policies, and practices related to personally-owned devices. Included in this guide is a chapter on access and infrastructure considerations for personally-owned devices. When published, the guide will be available on Alberta Education's website at http://education.alberta.ca/admin/technology/research.aspx.

Chapter 4 Security

This chapter illustrates a comprehensive, top-down view of securing a WLAN, beginning with high level policies, network elements, security aspects specific to WLANs, addressing laptop and client issues and URL filtering. All elements in this chapter correspond with a quality user experience while remaining diligent about managing risk.

In selecting WLAN hardware and management software infrastructure, it is best to choose APs that provide a comprehensive range of industry-proven security capabilities that integrate easily into any network design. WLAN hardware should provide standards-based authentication and encryption methods that satisfactorily address security concerns including authentication, NAC and data privacy. Additional layers of security such as VPN encryption should be strongly considered.

For very small school networks that function without a centralized RADIUS server for user authentication, some APs offer built-in RADIUS authentication. Your APs should integrate seamlessly with existing authentication systems, whether on existing school infrastructure or at the APs themselves.

4.1 Security Policy

Most districts are in the process of planning and deploying WLANs at school sites. It is vital to take steps to lock down wireless networks by implementing written policies to guide users and administrators alike. Create a wireless LAN security policy now. It is the foundation of running a secure WLAN. If a policy is already in place, review and expand this policy to ensure it encompasses wireless devices.

Which areas should a wireless LAN security policy address? At the minimum, it should focus on seven key areas that establish the basis for deployment, use, and management of wireless networks. Details of each key area are as follows.

1. **Define user base**

Clearly identify who can use the WLAN and what level of access each particular group of users will have to both the intranet and the Internet. One consideration is to compare to the existing wired setup and policy to goals of the new WLAN deployment. One way is choosing to simply block a particular user group's wireless subnet from the intranet.

Regardless of how access is granted, it is essential to determine the scope of access. More important, clearly define this in written policies and implementation practices.

2. **Identify appropriate usage**

After identifying the wireless network user community, identify the type of information that users can and cannot send over the wireless network. For example, prohibit sending personal information via the WLAN. In addition, prohibit ad hoc connections (i.e., peer-to-peer). Otherwise, savvy users could extend the network to users who do not have authorization to access the WLAN.

3. **Prepare for secure installation**

Identify specifically which internal department and named individuals are responsible for deploying wireless within the network. Define minimum physical security standards for AP locations, and determine who will have physical access to the APs. Ideally, try to place APs in controlled areas on the interior walls of the school. Adjust their coverage zone to the limits of your physical boundary, and not beyond, especially not into public areas like the road or parking lot.

4. **Establish wireless security standards for the district**

Define the minimum security measures enabled on all APs. Disable the service set identifier (SSID) broadcast feature, and change the default SSID to something that does not reveal a school or district's name. Enable one of the strongest current available methods of wireless authentication and encryption as outlined in Section 2.2 Wireless Security Standards.

Check compatibility of WLAN NIC utilities. If disabling SSID broadcasts on APs, some systems may not be able to connect as desired.

5. **Outline a contingency plan for loss of equipment**

If losses occur, the policy should stipulate immediately changing all the security settings within the wireless network (e.g., passwords and encryption keys). Best practices dictate to not store data on mobile devices, however should any data be on the devices, end-point security measures should be included. Treat any loss as a compromise of the system, and identify specific steps to take to mitigate further damage.

6. **Plan appropriate training of both staff and users**

Address training issues for the entire IT department as well as users to prepare everyone for the deployment, use, management, security, and incident response of the WLAN. Many districts often overlook this step during a new deployment. WLANs are completely different than conventional wired LANs. Outline a minimum training requirement, and develop a knowledge base for WLAN use from current successful implementations. Ensure that all staff are current on WLAN best practices.

7. **Establish guidelines for management and monitoring**

Once the wireless network has been deployed and locked down, there is no guarantee it will stay that way. The wireless section of a comprehensive security policy should define the frequency and scale of security assessments, which should take place on a regular basis to ensure continuity.

4.2 Network Security

Network Based Firewalls and Traffic Topology

Firewalls are essential at both the school site and district head office. If school sites access the Internet directly and do not follow a hub and spoke traffic topology, it is absolutely essential to employ firewalls. Most firewalls today have bundled security features such as VPN capability. Firewall should be deployed to protect critical network servers not only from external Internet traffic, but even more importantly to protect against internal unauthorized access attempts by users. Installing firewalls at both the school and district level will allow for any outbreaks or threats to the entire network to be isolated quickly.

Firewalls should be installed to protect entry points and network perimeters. Ideally they should also have IDP/IDS (Intrusion Detection and Prevention) capability.

There are essentially two different methods of schools accessing the Internet. Schools' WLANs access the Internet directly whether via an Internet Service Provider (ISP) like Shaw or Telus, or via SuperNet. As well, schools access the Internet via the district head office, referred to as a hub and spoke topology. The differences are how much firewall and security capability is at each school location, and aggregate bandwidth requirements for centralized traffic and control from the district level. Either method can be secure and functional. A district's current investments should be analyzed here to determine the best way to leverage investments already made.

If using the distributed method of each school accessing the Internet directly and not routing traffic through the district office, it is strongly recommended to use centrally manageable security appliances. Push central policy settings to managed appliances such as Fortinet or Check Point at school sites over the district's Internet connection. Several business-class network appliance providers offer products that combine VPN, WLAN (including WPA2), firewalling, URL filtering, VLANs and NAC support (see Table 10). Additional software is often required to augment and provide greater functionality, such as reporting on individual users URL attempts or more granular spam and virus management.

Table 10 - Firewall Vendors and Products

Vendor	Product	Gateway Anti-Virus	Integrated WLAN	Other
Check Point	Safe @ Office500W , UTM-1	Yes	802.11a/b/g, Super G, XR, WMM, 802.11n (on UTM-1)	Can support four VLAN security zones. 5, 25 or unlimited user versions available
Juniper Networks (acquired Netscreen Technologies)	AX series (Wi-Fi)	Yes	802.11a/b/g	Firewalls, IDS, IDP and other services are offered on separate stand-alone devices
Fortinet	60C wi-fi (actually has several products. This one and the 50C would be an entry-level ones)	Yes	802.11a/b/g/(n 60C only)	Launched by founder of Netscreen Technologies
Aruba	AP-41 AP-65	No, (integrates with Fortinet)	802.11a/b/g	A leading smaller vendor with solid solutions for K-12
Cisco	Aironet 1260 and 3500 series (Several high-end models also available)	No	802.11a/b/g and dual mode WMM	Largest company in terms of revenues, number of deployments and history. The overall market leader.
Watchguard	XTM-21, 22, 23 (W)	By subscription	W series only	
Barracuda	F101, F201, F301 (cellular support available on all models)		Only on models ending with the number "1"	Leading supporter of SSL VPN client access

These products range in price from $250 to $1,500, which makes them affordable to implement at individual school sites. IT budget managers must recognize that these devices will simplify remote support and will automatically reduce vulnerabilities because they accept and enforce central security policies. Should students access the Internet at school, or connect to the school's network from home, the security features, including URL filtering, are driven by these devices.

Under the other school of thought, implementing a centralized hub-and-spoke model allows for superior equipment to be implemented at district head office. The vendor licensing agreements will reflect pricing levels of the number of schools and throughput connecting to the Internet via your firewall. Speed will be another element for consolidation, and the district head office will need to have one or multiple managed SuperNet connections from Axia in order to handle the consolidated traffic from all schools.

Quality of Service (QoS) and Integration of VoIP

For data centric or data only networks, QoS is not a large factor or time consuming activity in optimizing wireless networks. The move to allow or carry more time sensitive traffic becomes commonplace in WLANs. Different enterprises have unique needs when it comes to traffic that would take advantage of QoS. In WLAN system planning, the QoS is specified in standard 802.11e. Some of the questions that need to be addressed for applications that require QoS are; what minimum bandwidth is required and what is the maximum latency that the application will tolerate? Below are some of the more typical time sensitive applications and their requirements.

Table 11 – Requirements of Time Sensitive Applications

Application	Data Rate	Latency
Voice	<32Kbs	<50ms
Gaming	32Kbs to 128Kbs	<10ms
CD Audio	64Kbs to 1.5 Mbs	High tolerance
Video HD	20Mbs	Medium tolerance

One school of thought is that designing a network for voice means not having to worry about data. Many companies though, take their already designed wireless data networks and attempt to overlay voice traffic on it. Several items to consider for these applications are:

- Handsets for voice are still only 802.11g capable which will have an overall throughput effect on a 802.11n data network.
- Voice traffic is the most likely to find the coverage holes in a network.
  - Users are used to the operation and convenience of smart phones.
  - Users will not disconnect a call to use a stairwell or elevator.
- Users will be roaming across cell boundaries during a call.
  - The handset during this time will be using the lowest rate allowed because they are the farthest away from the AP- 6.0Mbs.
  - This affects all other throughput during this session on this AP.
- The network administrator will find out if the cell boundaries are in the correct location to provide seamless roaming.

Virtual Private Networks (VPN) and Proxy Servers

Configuring VPNs to communicate between schools and head office is critical for ensuring the traffic integrity. VPN client software can then be deployed on student systems allowing remote, after-hours access to resources they need to complete homework. This is an excellent way to enforce students' Internet access while not on school premises to flow through school or district resources, and thus be monitored and protected in line with the security policy. Students would be able to use the Internet and resources exactly as if they were physically at school.

There are proxy server solutions which could address basic Internet traffic management of off-site students, however, these are not as capable of monitoring and managing as a VPN solution. One example would be simple access to files or centralized/hosted resources.

Intrusion Detection and Prevention (IDS/IDP)

Deploying network wide IDS/IDP (including WLAN IDS/IDP) is the most secure. This protects the network from attack attempts and can provide an alert in the event of unauthorized activity. Logs and analysis of how users attempt to gain access to the network can be compiled. This data can be used in future network upgrades and designs.

It is recommended that at minimum a WLAN Intrusion Detection System (IDS) or an integrated intrusion detection and prevention solution. The latter not only identifies intrusions, but also addresses them automatically.

Virtual Local Area Networks (VLANs)

Isolating different user types (grouped by their functional requirements) into VLAN network segments and firewalling between VLANs will greatly increase security. Furthermore, isolated users may only access exactly the resources they require, which helps with overall IT resource management and decreased support requirements. Different user types or groups are isolated from one another for further protection of peer-to-peer breaches.

As WLANs scale out to accommodate more users, VLANs also isolate network traffic to help control and reduce bottlenecks associated with large, flat networks. As application adoption and usage increases, this management technique will provide maximum control of bandwidth, and ultimately cost.

4.3 Wireless Security

Because of the nature of wireless signals, it is impossible to stop anyone within the signal range from attempting to access data or the entire WLAN. This is the nature of wireless technology. Fortunately, there are security methods available today to address these security concerns. It is typically a matter of policy, will and budget.

In reality, not all WLANs are configured and deployed in an ideal manner with secure access and authentication. As such, one of the main issues with WLANs is unauthorized access to network resources and unnecessary traffic. The following will help identify common pitfalls and associated challenges in wireless security.

Avoiding Common Wireless Security Oversights

Here are the most common security oversights and how to avoid them.

1. **Breached Firewalls**

   Most schools have firewalls around the network, wireless or not, and rightly so. However, if the configuration does not isolate the wireless network from firewalled resources, then the level of control diminishes. Make sure it does, otherwise there is no barrier (the entire point of the the firewall) should an unauthorized user acquire wireless access.

2. **Spurned Media Access Control (MAC)**

   MAC is often ignored because it is not spoof-proof. It should be considered another brick in a district's overall security strategy. It is essentially another address filter, and it clogs up the works of a potential hacker. It limits network access to registered devices that are identified on address-based access control databases.

   When MAC is in place, the intruder must bump into it before even realizing it is there, and then attempt to get past it, making the intruder known. A MAC list creates three classes of visitors. First, friendly entities are on the MAC's list; second, unknown entities that are not on the list and who knock by mistake; and third, entities who are not on the list but are known because they have tried to get in before, uninvited, and are now instantly identifiable if they approach again.

   MAC address filtering directs the AP or a RADIUS server configured with the MAC addresses of the permitted wireless clients to be granted access. Unfortunately, this method by itself is not secure because frames could be sniffed to discover a valid MAC address, which the hacker could then spoof.

   WLANs require the same security policies as wired networks, but it takes more steps to get there. The same issues that are of concern in the wired world should still be of concern with WLANs and devices. Keep encryption strong, keep certificates in place and manage security in an ongoing fashion. Wireless security is not a matter of different security; it is a matter of more security.

3. **Use the highest level of authorization and encryption**

   Refer to Section 2.2. This is often the weakest link in a wireless security infrastructure, but it can be addressed through the use of continually updated best practices.

4. **Allowing unauthorized (rogue) APs**

   Have a procedure in place for noting the presence of neighbouring APs and a policy of how to deal with newly discovered rogue APs on the wireless network.

5. **Permitting ad-hoc laptop communication**

This is difficult to enforce in any environment. The ad-hoc mode lets Wi-Fi clients link directly to another nearby laptop, say from one student to another. As part of the 802.11 standard, ad hoc mode permits a laptop's NIC to operate in an independent basic service set configuration. This means that it can go peer-to-peer with another laptop via RF. Note that this permits access to the entire hard drive of the laptop.

Be aware of potential new applications being pitched for deployment on the WLAN if they require any sort of peer-to-peer element. These applications should be rejected from the highest level of the security policy.

6. **Not Protecting Legacy WLAN Investments**

The best answer for legacy WLAN equipment is to replace it. If that is not feasible, then it should be isolated on a separate network with firewall separation or virtual LAN (VLAN) that blocks access to other school or district resources. Only the expected data should be allowed to flow, and only to a pre-authorized address and/or gateway.

If the devices do not support reasonably strong legacy wireless security, but can support a VPN, then the VPN should be activated, and security settings should be made as strong as possible. VPNs run independently of the WLAN and are immune to weaknesses in the wireless security protocols. If users need to roam, this option will prove difficult with the Internet Protocol security, because it does not tolerate interruptions and IP address changes. Secure Sockets Layer (SSL) VPNs and proprietary mobile VPNs can support roaming where required.

Data traffic and applications allowed to run over the legacy wireless system should be limited. Bar access to unnecessary network resources and applications.

Migrate to Wi-Fi Protected Access 2 (WPA2) compatible WLAN network interface cards, drivers, supplicants and APs for all new purchases.

Network Access Control (NAC)

Wired networks can be protected by physical means with walls and doors with locks. Wireless networks use radio waves to move data, and therefore, anybody can easily receive and transmit radio waves to gain unwanted entry to the network. Network access control (NAC) is used to limit that unauthorized access.

In an educational environment, device types range widely from Windows, Mac, or Linux machines; laptops; desktops; personal digital assistants (PDAs); tablet PCs; and perhaps even wireless IP phones. Maintaining network resource availability and integrity becomes a challenge in this open and heterogeneous environment. Network access control (NAC) recognizes users, their devices, and their roles in the network as per the organization's security policies.

Security policies may define a simple user password authentication process, no device authentication and unlimited access once authorized on one end to comprehensive policy enforcement on the other. A comprehensive policy related to network access includes: user authentication, role-based access control (RBAC) and device authentication.

User Authentication

Typical wireless user authentication is done using protocols and/or services, such as Kerberos, Lightweight Directory Access Protocol (LDAP), RADIUS, SQL and Active Directory.

Role-Based Access Control (RBAC)

Administrators can maintain multiple user profiles with different permission levels by using RBAC. Typical school district roles would be administrative staff, faculty, students, IT staff and guests. With RBAC, each role receives a different level of network access and permission.

Wireless Device Authentication

With personally-owned devices seeking access to the network; viruses and already compromised machines could wreck havoc to an otherwise secure network. With NAC, machines requesting access can be queried for compliance with security policies, recent updates and vulnerabilities before being allowed on the network.

Major NAC hardware Components

Wireless Access Points (AP) and WLAN

Wireless APs can be autonomous or WLAN access controller-based, also known as fat and thin APs respectively. In the autonomous architecture, the fat APs completely implement and terminate the 802.11 function. The AP bridges traffic between the wired and wireless interfaces. Each AP is independently managed. The downside is complexity. Fat APs are intended to be stand alone and are expensive to install and maintain. Nevertheless, the devices have uses in smaller network installations.

The centralized architecture using thin APs involves a WLAN access controller that is responsible for the APs' configuration, control and management. The 802.11 function is split between the AP and the access controller. This architecture is scalable and therefore suitable for larger implementations.

Authentication servers

Authentication servers come in many varieties. The authentication software can reside in an AP, server, router or other piece of hardware. However implemented, the term authentication server is used to refer to the combination of hardware and software that fulfills the authentication function.

In addition to variations in hardware, there are different logical algorithms used by an authentication server. The major authentication algorithms utilized are basic password lookup, Kerberos, RADIUS and public key encryption and can be used singularly and in combination. Design choices are dependent on the existing and planned infrastructure, scalability requirements and security policies.

User Database

Basic authentication uses text files to store the authentication information. On average, half of the file needs to be read before a user record is found. Not an issue for small sets of users; however, for large numbers of users the lookup process becomes unacceptably slow.

An alternative is to use a database. Databases are optimized for looking up information in a very large data set. RADIUS servers are specialized to do this; or they can refer to external sources such as SQL, Kerberos, LDAP or Active Directory servers to verify the user's credentials.

Public Key Infrastructure (PKI)

Public Key Infrastructure is a set of hardware, software and procedures needed to create, manage and distribute digital certificates. The certificates can be used to verify that a public key belongs to an individual.

Router and Switches

Both are LAN devices that process the frames sent from the APs. Switches at Layer 2 maintain the VLAN information to keep traffic separate. Routers at Layer 3 move packets between VLANs or networks according to security policies implemented via Access Control Lists.

Authentication Protocol Requirements

802.1X in wireless is currently the de facto standard for secure authentication and key exchange in enterprise environments. 802.1X is based on the Extensible Authentication Protocol (EAP), and offers several methods to protect authentication exchanges as described earlier under the "EAP & 802.1X Authentication Protocols" section. Many protocols have been developed but these three are popular for use with EAP and wireless LANs:

- EAP-Transport Layer Security (EAP-TLS)
- Tunneled Transport Layer Security (TTLS)
- Protected EAP (PEAP) has different versions but most supported is EAP-PEAPv0/MSCHAPv2

Table 12 – TLS Based Authentication Methods Comparison

	EAP-Transport Layer Security (EAP-TLS)	**Tunneled Transport Layer Security (TTLS)**	**PEAP (EAP-PEAPv0/MSCHAPv2)**
Client implementations	Cisco, Funk, Meetinghouse, Microsoft, Open1X (open source)	Funk, Alfa-Ariss, Meetinghouse, Proxim, Avaya, Enterasys	Cisco, Microsoft, Funk, Meetinghouse
Supported client platforms	Linux, Mac OS X, Windows	Linux, Mac OS X, Windows	Linux, MacOS X, Windows
Authentication server implementations	Cisco ACS, Funk Odyssey, Interlink Secure.XS, Meetinghouse AEGIS, Microsoft IAS, FreeRADIUS	Funk Odyssey, Interlink Secure.XS, Meetinghouse AEGIS	Cisco ACS, Microsoft IAS, Interlink Secure.XS, Meetinghouse, Funk
Authentication methods	X.509 Certificates only	CHAP, PAP, MS-CHAP, MS-CHAPv2, and EAP methods	Different versions, most supported is PEAPv0/MS-CHAPv2
Pros	EAP-TLS is an IETF open standard and well-supported among wireless vendors. Extremely secure authentication method. It is the strongest 802.1X authentication method currently available. If a PKI solution is already in place, this can be leveraged for an easier implementation.	Can use an existing infrastructure of user certificates, such as Windows Domain Controllers, SQL or LDAP databases, or token systems. Does not require a certificate infrastructure for the endpoints. Only the authentication server (RADIUS) needs a certificate to leverage PEAP.	EAP-PEAPv0/MSCHAPv2 is a popular choice because it is natively supported by Windows. Also supported by Linux and MAC. Can use an existing infrastructure of user certificates, such as Windows Domain Controllers, SQL or LDAP databases, or token systems. Does not require a certificate infrastructure for the endpoints. Only the authentication server

		Does not require a significant change in the infrastructure.	(RADIUS) needs a certificate to leverage PEAP. Does not require a significant change in the infrastructure.
Cons	Maintain a certificate infrastructure for all of its users. This is a major undertaking if a certificate system is not already in place.	Not typically supported natively by the client OS. Requires third-party client software.	Not as strong authentication as TTLS or TLS.
Best use	High security environments with a PKI certificate structure and key management with enterprise owned and managed endpoints.	Medium to high security environments.	Medium to high security environments.

With security policies as a backdrop and guide, a necessary initial decision is if the cost and complexity of issuing client certificates is warranted. If a PKI already exists, the tasks for a wireless LAN deployment with EAP-TLS are easier. However, organizations which have not already deployed PKI should consider TTLS or PEAP instead. The authentication method choice is important as it will drive all future product choices.

Once that initial decision is made, the next important consideration is to ensure that the RADIUS server, access point and client software are compatible, and that 802.1X and the EAP method chosen are supported by all three devices.

802.1X with Web-Auth (Captive Portal)

To support non-managed devices or devices that do not support 802.1x, a guest's web-based authentication, also called captive portal, can be used. With captive portals, users must enter their username and password via a web page before being permitted on the network. The advantage of this is that no configuration is required for the endpoint; all a user needs is access to a web browser. However, it is inherently less secure than 802.1x. Security can be increased by combining different products. Some captive portal systems are inelegant.

NAC with automated compliance enforcement

Although typically not incorporated in an academic environment, more comprehensive NAC systems are available and are included here for completeness. Using predefined policies, devices are checked for critical operating system updates, antivirus software virus definition updates and antispyware definition updates. These scans can be done for Windows, Mac OS and Linux-based operating systems and machines, as well as non-PC networked devices such as PDAs, printers and IP phones. Noncompliant machines are redirected into a quarantine area, where remediation servers can provide operating system patches and updates, virus definition files, etc. Numerous vendors such as Cisco, Infoexpress, Juniper, Bradford Networks McAfee, Forescout, Check Point and Sophos supply end point security products.

Implementation Scenarios

Some examples follow, moving from one level to the next represents an increase in the number of users and security stance. The levels themselves are arbitrary.

Level 1 implementation
Scalability is not paramount in small wireless implementations, hence components required are reduced. Fat wireless APs, LAN switches and routers suffice for a small implementation with few users. Also, smaller organizations typically lack the expertise or resources to implement and manage a PKI infrastructure.

At this level, the AP can act as the authentication server and simply store a list of valid user names and passwords, and only authenticate users according to this list.

Service Set Identifiers (SSID) and VLANs are used to segregate users and ACLs to limit access to network resources. SSIDs, VLANs and ACLs are relatively easy to set up and are supported by the major LAN equipment providers.

Level 2 implementation

Centralized WLAN networks with WLAN access controllers offer greater scalability than a network of distributed fat APs. Access controllers can scale to support hundreds of APs. PEAP or TTLS is suggested at this level as these methods only require certificates on the authentication server. A third party certificate service could supply the needed authentication server certificates, and a PKI implementation would not be needed. Additionally, a RADIUS Authentication Server communicating with a database would be required. Fortunately, there are many ways to do this.

Level 3 implementation

Level 3 builds on the same Level 2 principles, but Level 3 is a more rigorous and secure implementation. A dedicated PKI Certificate Authority infrastructure is required with the EAP-TLS authentication method. In addition, a client remediation service is incorporated into the network to verify that the client meets the required security stance. Should the device fail the security check, it would be placed in quarantine and updated with the required patches and anti-virus signature files. If the remediation is successful then the device would be allowed to access network resources. The role based access control system implemented offers not only user authentication but also authorization based on the configured role. Each role has different permission levels limiting access to devices or services.

Ensure guest access credentials expire on a daily basis, or more frequently as needed. Guest access should be treated like a sign-in sign-out sheet, and should be expired as soon as it is no longer needed.

4.4 Mobile Host Security

Mobile host security means securing the laptops and other devices that come on and off of a school's WLAN. This is accomplished with a broad mix of technology and best practices of users complying with a sound wireless security policy.

Introducing mobile computers onto a network on a large scale will impact security. They move from network to network and their exposure to vulnerabilities while outside of the school WLAN are unknown. They can be physically compromised and data can be stolen.

Security Software and Operating System Updates

Desktop and laptop patch management should be deployed to ensure the latest product patches are pushed to all clients. This will help to increase security, reduce compatibility challenges, keep interfaces consistent and decrease support costs over time.

Have a comprehensive desktop management strategy that includes all mobile devices and laptops. A comprehensive, centralized dashboard to monitor, maintain, manage and report on all desktop management aspects. Do not settle for just patch management software. The feature and functionality set of the chosen management system should be comprehensive and in one simple Graphical User Interface (GUI).

Personal Firewalls

Personal firewall software should be deployed on each and every laptop. Ideally, these software firewalls will function within a centrally controlled system that can enforce usage with and is compatible with hardware firewalls.

All laptops with a wireless NIC must have a personal firewall installed that supports connection-specific policies. As laptops are often outside the protection of the school or district firewall, every laptop should have a personal firewall installed. This will be critical for students taking their laptops home and then returning, with potential infections, to the school WLAN. The firewall built into Vista may provide sufficient baseline security for student laptop use, although software client licenses compatible with firewall solutions at either the school site or district head office is better. What is built into Windows XP is not sufficient. The personal firewall should be configured to block split tunnelling and any ad hoc WLAN connections.

Anti-Virus (A/V)

A/V protects and minimizes threats, and is essential for all laptops because new viruses proliferate daily and spread quickly. A/V should be centrally controlled so the definitions can be monitored. If not, definitions may not be updated and laptops would eventually get a virus. MacAfee, Symantec, Trend Micro, Computer Associates and many other vendors have central control and monitoring.

Despite offerings for stand alone, typically consumer versions, do not implement these as they do not have central management and require maintenance and updates. Some small districts may have this in place on guest or even existing legacy laptops accessing their WLANs.

Anti-Spyware (A/S)

A/S protects against threats through the Internet browser. Protecting against this will dramatically reduce the level one technical support requirements and support time and costs. Fewer users asking to have their system cleaned allows for more time for other projects or additional training.

Pop-ups can be frustrating and will impact a user's experience. A/S can protect against these as well.

Encrypted File Systems (EFS)

Security certificates and critical data will be accessible to a savvy user who happens to come across a lost or stolen laptop, and includes all access settings to the WLAN and other resources including applications, VPN and more. Using EFS, systems will make it challenging, if not impossible, even for a highly skilled user to crack and gain access without the user's network password. In this scenario, password policy and enforcement is critical.

The key to address here is that if a laptop is lost, no one could access the data on it.

4.5 Content Security

The scope of content security typically covers the following:

1. Website surfing content control (i.e. filtering unacceptable URLs)
2. Controlling use of instant messaging applications
3. Controlling access to file sharing peer-to-peer (P2P) networks

Traffic between computers, APs, controllers, switches, firewalls and other network appliances can be controlled significantly by implementing content security policies and technology.

Features and specific functionality vary between vendors and types of technology solutions. Solutions can include blocking categories or websites (such as adult or gambling), ad-hoc white and black listing websites, keyword analysis and resolution (even if contained within an e-mail, instant message or websites) and more.

Solutions exist for both centralized and distributed control. Most firewalls released in the last year have integrated solutions that may be more cost effective then an entirely separate system. Centralized control is generally recommended as it eases administration burden and can give management high level reports of the entire organization's activity.

Used effectively in conjunction with a hub and spoke traffic topology, districts can control users' content while they are on the school WLAN or using their laptops while on another network.

Some sample vendors in this space include:

- www.symantec.com
- www.8e6.com
- www.fortinet.com
- www.checkpoint.com
- www.barracudanetworks.com
- www.bluecoat.com
-

These types of solutions are only as good as they are configured and installed in line with the vendor-specific feature set. Often, there is a channel partner, consultant or even an existing value added reseller who may be a better first line of communication and sales for these content security solutions.

Chapter 5 Innovation and Issues

5.1 Wireless Gigabit Alliance (Wi-Gig)

As 802.11 matured into 802.11a/b/g/n with new spectrum and additional data rates and services, Wi-Gig is looking to utilize the 60 GHz band with data speeds up to 7 Gb/s. Working with the Wi-Fi Alliance, which does interoperability testing for 802.11 devices, the Alliance hopes to leverage the existing 802.11n capabilities and allow migration to the Wi-Gig while maintaining backward compatibility with legacy 802.11 equipment. As many companies and enterprises are currently migrating their wireless systems from 802.11a and g to 802.11n, they will then be able to migrate at the appropriate time to the Wi-Gig technology. As data rates get faster, the opportunity to support a wider range of applications become commonplace, Data rates of 7 Gbs can support a wide range of multimedia applications simultaneously.

The Alliance has published its application specifications online at http://wirelessgigabitalliance.org/specifications/.

5.2 White-Fi

With the August 2011 switch to digital television, a portion of the radio spectrum previously occupied by those transmitters will become available for use. Some of that spectrum will be reserved for public safety, some will be auctioned off and some will be available for licensing for private use. With all the WLAN systems currently utilizing the unlicensed bands for Wi-Fi use, the most likely use of this licensed spectrum might be for a last mile broadband service. It would not appear to be a likely resource for a WLAN application as each device that uses a licensed spectrum pays a license fee, and with thousands of wireless devices currently on WLAN networks a migration to a Wi-Gig technology at some point in the future seems the more likely of scenarios.

5.3 Real Time Location Services (RTLS)

With school districts continuing to deploy wireless networks in schools, innovative ways of using this infrastructure are emerging. While some existing network management suites show the location of laptops, many industries are making use of the coverage and capacity of their WLAN to add RTLS to it. An RTLS solution can be used to track wireless clients and high value mobile assets anywhere there is WLAN coverage.

RTLS belongs to a family of applications covered by the term RFID. Assets can be tracked using tags that range in function from passive to active. Passive tags are nothing more than a microchip embedded onto an antenna substrate. These inexpensive tags are 802.11 radios with a battery and are designed to transmit on programmable intervals and send a signal to any AP within range. That very short message is forwarded to a device called a location appliance or engine. When it receives the message from the device via several APs, it will then triangulate the position of the device. With a software application that hosts facility maps, the location of any tagged asset can be tracked in an instant.

5.4 Health & Safety Concerns

The health and wellbeing of students is of the utmost importance to Alberta Education. The ministry continues to monitor available research around Wi-Fi safety to ensure that the latest information is available to school authorities and the general public. In addition to this WLAN Best Practices Guide to help school authorities safely and effectively install wireless networks, Alberta Education has developed and published the "Wireless Networks and Safety" fact sheet.

Alberta Education continues to rely on the medical and safety expertise of Health Canada and Alberta Health and Wellness to establish its guidelines for safety for students regarding exposure to low-powered RF signals in schools. Individual school authorities, however, have the ultimate responsibility for providing a safe and caring learning environment and as such are able to decide which technologies go into schools.

Appendix A Case Studies

Introduction

Wireless networks are becoming more and more common in Alberta school authorities. The following case studies were done to share their experiences and help all school authorities implement and manage their wireless networks. The case studies examine each school authority's particular concerns, challenges and decisions regarding cost, vendor selection, implementation, security, maintenance and support of their WLANs.

The Calgary Board of Education, Edmonton Public School Board, Calgary Catholic School District, Grand Prairie School District and Wolf Creek School District were all very generous and open about their experiences in implementing and managing WLANs, Both the Calgary Board of Education and Wolf Creek School District were part of the Emerge One-to-One Laptop Learning initiative.

Four years ago there was a considerable variety in the road maps that the districts took to begin implementing wireless technology. As wireless networks mature, it has become apparent that there is less uniqueness about the different networks. A wireless vendor that is in the enterprise class, controller-based typically has all the tools at their disposal to allow a school authority to deploy a secure, up-to-date and well managed network.

Calgary Board of Education (CBE)

The Calgary Board of Education (CBE) is the largest school authority in Alberta. It has allocated extensive resources to its IT infrastructure and its rollout of wireless is nearing completion. The original design provided a blend of coverage vs. capacity as needed. This system is a prime example of a system or systems moving from coverage to capacity model. Its redundant IT infrastructure is managed entirely in-house by more than 150 IT staff.

Cost Saving Techniques

The original partial Distributed Antennae System (DAS) implementation was a cost saving techniques and allowed the capacity to grow with the coverage. With the size of both the school authority and the deployment, it was able to put enough money aside as part of the capital project to properly cover all schools. The real issue that had been foreseen was the ongoing funding of operations. Wireless is more complex and less reliable than traditional wired technology and therefore requires more support. Also the wireless infrastructure needs to be maintained, broken parts replaced, controller OSs upgraded etc. Operating dollars were found to cover the equipment and maintenance costs, but not to fund the staffing. As such, they implemented the Airwave management system which helps in diagnosing problems and provides for easier management of the equipment, allowing them to be proactive.

Calgary Board of Education Summary

- *103,000 Students*
- *9,400 Staff*
- *230 Schools*
- *220 Complete Wireless Networks*
- *10 Partial Wireless Networks*
- *Aruba Solution. Wireless Controllers and Thin Access Points*
- *Over 150 IT staff*

Vendor Selection

The DAS that was left in place provided full coverage throughout the building; however it did not provide appropriate capacity. DAS is augmented by deploying additional 802.11n access points in a traditional configuration (APs placed in hallways, classrooms and open areas). This traditional configuration covers over 90% of the existing DAS deployment while providing approximately 10 times the capacity of the previous installation. DAS is still used provide coverage where it is cost prohibitive provide to deploy APs in the remaining 10% or where traditional access point.

Implementation

CBE still uses out-sourcing for the majority of its RF-related work, including antennas and installation. The balance of wireless network administration and maintenance is done in house.
The entire network, including ports to all end devices, is based on a 1 Gb/s. The CBE completed an upgrade project from 100Mb/s to 1 Gb/s in 2007. The cost difference between 100Mb/s and 1 Gb/s was nominal for service that provides the bandwidth necessary for an 802.11n capable wireless system.

Power over Ethernet (PoE) is used to power the APs in the closet, eliminating the need for more electrical outlet installations. Services such as storage, e-mail and content filtering are centralized in CBE's main network operations center (NOC). A redundant NOC is setup to provide failover services for their most critical systems. Full application redundancy is planned and some implementation is under way. CBE uses a Motto for wireless deployment of Demo, Capacity and Enhancements to provide at a glance visibility into the maturity of the system in any corner of its network.

Security

Guest wireless access at schools is directed to a captive portal and a temporary account can be obtained for specific time duration. Student wireless traffic is also routed through a captive portal for access and authentication. With current controller based technology, the ability to provide unique SSIDs at the network edge for specific network resource access allows the VLAN to be rolled to the network edge by matching it with an SSID. All content filtering is done at one central location.

Non-CBE devices are isolated on their own wireless network and their traffic flows straight out to the Internet from the school's connection without going through the district head office hub-and-spoke configuration. All internal network access is restricted to CBE-owned devices only. WPA2 is implemented for security. Content filtering and anti-virus solutions are deployed to protect end users.

Maintenance and Support

CBE employs over 80 IT staff to support the schools and about another 80 staff to support the head office and data centers. The NOC group consists of four staff. Together, they support more than 40,000 devices. It does not outsource maintenance or support and prefers to use the existing staff to perform all the work.

Senior high schools have a resident (dedicated) technician while multiple junior high schools and elementary schools are supported by sharing technicians (each site is allocated a technician for a part of the week). Some staff at the schools are junior and do not work with servers. Only senior administrators are allowed to maintain the servers and sometimes they are required to support multiple schools, both remotely and onsite. The first line of support is the teachers themselves. Students can speak to teachers, who in turn call the help desk to initiate a support request.

For the wireless portion of the network, now that they are nearly fully deployed, the project they will need two people to maintain the system, and would likely require a third if it were not for the Airwave system. Funding for the two additional staff in this difficult budget cycle has not granted and providing the required attention to the wireless system has impacted other IT operations. This is an ongoing area of concern.

Lifecycle

The anticipated life cycle plan for the hardware is three to five years for APs and five to seven years for wireless controllers. District-owned wireless client devices typically have an evergreen cycle of four to five years, depending on the device.

Conclusion

CBE has put a tremendous amount of thought and planning into its wireless network solution. Its IT staff is highly organized and committed, and this is reflected in the design, implementation and operation of the entire enterprise network.

Calgary Catholic School District

The Calgary Catholic School District is one of the largest school authorities in Alberta. It has already installed wireless networks in 106 schools effectively tripling its wireless network coverage in the past four years.

Calgary Catholic School District Summary

- *45,000 Students*
- *5,000 Staff*
- *106 Schools*
- *35 Complete Wireless Networks*
- *72 Partial Wireless Networks*
- *Aruba Solution. Wireless Controllers and Thin Access Points*

Cost Saving Techniques

Calgary Catholic still maintains an approach that provides coverage then capacity. This allows a steady growth of infrastructure. By monitoring the network carefully as it grows, coverage then capacity can be deployed as a particular school or site warrants.

This creates a manageable system implementation as AP purchases can be spread across budget cycles, and is a sustainable growth pattern for IT staff.

Another example of time intensive work that takes away in-house support staff time is the ongoing support of firewalls, anti-virus software and spam filtering systems.

Vendor Selection

Calgary Catholic uses Aruba for its wireless solution, 3Com/HP for its switching and routing platform and CheckPoint for its firewall environment.

Calgary Catholic has created what it calls "a three-way partnership" with the reseller and the manufacturer whereby they both provide support, guidance and planning for the board's entire IT infrastructure. This provides the school authority with access to industry experts through an existing strong relationship when it is looking to embark on complicated IT projects and ensures that the reseller has direct access to support from the manufacturer of the hardware. For wireless networks, centralized management was a key criterion for selecting Aruba as its vendor.

Implementation

The roll-out of the wireless networks consists of a coverage then capacity rollout. Only a portion of the network is currently "n" deployed. By using the Airwave Management Utility from Aruba, IT staff can plan, budget and implement "n" technology and add APs to provide capacity as necessary. All APs are powered via Power over Ethernet (PoE).

A challenge it faces today in its implementation is that when all the students are in the hallways between classes or on their way outdoors, the wireless signal is negatively affected. It also discovered that with the increase of users on the network, it had to upgrade the backbone switch inter-connects from 100Mb/s to 1 Gigabit to handle the traffic loads.

All control and configuration is centralized to head office via SuperNet. This eases management of the networks and provides greater cost savings overall and an increase in control of IT. A wireless pilot was conducted at one high school. The school was outfitted with "n" APs throughout, and students used laptops purchased through the school or their own devices to connect to the network. This program was a great success and may well be the model of the network road map.

Security

From each school, user traffic is routed back through the head office firewall for centralized content filtering. Packet shaping and compression is handled at the school level to minimize the traffic impact with this solution. Checkpoint is the firewall product used.

Guest access is limited to a 6 AM to 11 PM time window. Administrators and students use an 802.1x authentication protocol to gain network access and all visitor access is via a captive portal. War driving (the process of driving around with laptops to find wireless networks) is always a concern. All APs are tuned so that their signal does not transmit outside building walls. The Aruba solution automatically detects rogue APs should any be brought into the environment.

Maintenance and Support

In-house support is covered not only by a head office help desk but by administrators at the school level. Calgary Catholic has 20 school level IT administrators. Technicians are setup by region to balance the workload. Centralization of services and data lowers the complexity of networks and lowers the time required to maintain those systems.

Out-sourcing is primarily related to installation of equipment. About 25% of installation is done by outside contractors.

Lifecycle

With the Aruba hardware having a lifetime warranty the lifetime of the systems may depend more on new technology releases and adoption. The current “n” APs have an expected lifecycle of three to five years. With the system continuing to grow methodically that will spread the lifecycle replacement program as well.

Conclusion

Calgary Catholic’s network is a great example of a well run network of substantial size maintained on a very strict budget by a relatively small team of IT professionals. By purchasing standard hardware from major vendors and maintaining support contracts, it is able to keep support costs at a minimum while gaining access to industry experts.

Edmonton Public School District (EPSD)

Edmonton Public School District (EPSD) is the second largest school authority in Alberta. Some of the schools have chosen a hotspot deployment strategy that accounts for the approximations in the summary. In 2006, wireless was installed in a few schools. Each school had a few dozen school-owned devices. As of 2011, wireless is an essential means of connecting at many of the schools. Currently, Edmonton Public's Aruba Airwave Wireless Management Suite indicates around 11,000 unique users per day connecting to the network.

Edmonton Public Schools Summary

- *80,000 Students*
- *7600 Staff*
- *197 Schools*
- *≈ 110 Complete Wireless Networks*
- *≈24 Partial Wireless Networks*
- *Aruba Solution. Wireless Switches and Thin Access Points*
- *48 IT Support Staff*

Cost Saving Techniques

Edmonton Public has found that doing complete site installations has worked out to be a cost saving for them. The infrastructure time and electrical work for network cabling and PoE planning has been minimized. Planning based on using the 5GHz band to deliver higher capacity requires more APs be installed. However, working with a product that is scalable and does real time channel and power planning reduces costly and time consuming site surveys. Newer software from the vendor has allowed them to transition to a centralized controller that is providing a cost savings due to a reduction in the number of site based controllers. The Airwave Wireless Management Suite has allowed for detailed troubleshooting and asset management to reduce costs.

Vendor Selection

Aruba has been chosen as the wireless vendor, HP for school core switching and routing and Fortinet for firewall technology.

Implementation

Since November 2009, all APs being deployed are dual radio 802.11n capable. An AP per classroom and one for coverage in open areas like gymnasiums, staffrooms, and libraries was the chosen method. Aruba's Adaptive Radio Management is utilized to optimize channel and power settings per AP at the site. PoE has been the norm for installation and a migration to Gigabit backhauls to support the new 802.11n access points. A commitment to upgrade the physical wiring to a CAT6 matches the high throughput of 802.11n and Gigabit backhauls Legacy wireless 802.11 a/b/g access points are still supported by 10/100 PoE switching architecture on CAT5 cabling in some cases.

Accommodating the increasing number of personally-owned devices requires higher density deployments. IP addressing continues to be a challenge to keep from exhausting IP pools. Large numbers of personally-owned 802.11g devices are crowding the 2.4 GHz band. Recommendations for school-owned laptops and netbooks are that they be dual band capable in order to utilize the 5.0 GHz spectrum.

Security

Security is handled at several levels in Edmonton Public's system. With wireless segmentation at the AP level and content filtering at both the local controller as well as Internet egress location.

Maintenance and Support

The long term goal for Edmonton Public's IT staff is that wireless will simply become one more technical package that the staff deploys and supports. Initially, wireless was managed in isolation with stand alone wireless management tools and utilities. There is always a steep learning curve when it comes to deploying new technology, especially one that is now as entrenched as wireless. Originally there were several departments that each played a role in the wireless deployment. Working more closely together and getting vendor training for their network has provided the background for a solid support team and strategy.

Lifecycle

The life cycle of a server is three years, five years for desktops and three to four years for laptops. Networking is typically a longer seven year plus cycle.

Conclusion

IT staff supporting Edmonton Public's wireless network attend conferences and training. They are mentoring their field support staff so that wireless knowledge is shared within the department. They have used visual workflows for field technicians to allow them to communicate directly with stakeholders. They have a product that is performing to expectations. Plans for the future are to continue to roll out more wireless networks to more schools.

Wolf Creek School District

Wolf Creek School Division is a smaller school authority located in Central Alberta with its division office located in Ponoka, Alberta. The district is part way along its road map to complete wireless coverage in all schools. It has used an Alcatel branded Aruba solution for the vendor choice and with their switching and routing hardware from the same vendor, it has provided a one-stop experience for network related hardware.

Wolf Creek School District Summary

- *7,200 Students*
- *900 Staff*
- *26 Schools*
- *20 Complete Wireless Networks*
- *6 Partial Wireless Networks*
- *Alcatel branded Aruba Solution. Wireless Controllers and Thin Access Points*
- *9 IT staff*

Cost Saving Techniques

Wolf Creek's wireless implementation is focused around a vision for excellent learning environments. To ensure that budget challenges do not compromise project outcomes, it maintains a technology reserve that can be used to ensure that the learning environment is not compromised. Wolf Creek is continually on the lookout for efficiencies and cost saving opportunities. One area recommended by the vendor was the choice of AP for the implementation. Without effectively compromising range or capacity and still providing 802.11n system wide capability, the installation achieved cost savings.

Vendor Selection

Wolf Creek uses an Alcatel branded Aruba solution for its wireless equipment and Alcatel- Lucent equipment throughout its enterprise. All switches provide Gigabit PoE to the wireless APs and with the district's choice of AP, it can utilize 802.3af PoE instead of the higher power PoE required by some APs.

Implementation

Wolf Creek handles the majority of its system design and installation and maintenance in-house with approximately 10% of the system design by outside contractors. By the time of this documents publishing, wireless should be close to 90% rolled out, with 23 of the 26 schools complete.

Security

Content filtering is done on a per school basis. The system provides a complete range of role based wireless access control. There are four possible wireless SSIDs available to users. Guest access utilizes a captive portal and one of the temporary accounts that each school has access to. Access to internal servers and resources is not allowed and guest devices are not permitted to communicate with one another while connected to the Guest network. The Secure network is reserved for Wolf Creek's managed domain member devices. Login is the same for a wired as a wired device and access to all network resources is provided. They utilize two other SSIDs in the network, one for presenter use that may require raw Internet access; the devices are isolated and have a separate connection to the internet. The other is a DMZ that requires a two stage process which allows for a Host integrity check prior to allowing the device network resources. The integrity check process is accomplished using InfoExpress CyberGatekeeper appliances and desktop agents. There are various stages of auditing here and options by the user to not take advantage of these device audits which immediately places him into a guest user role.

Maintenance and Support

With nine technical staff, a careful balance is required when implementing new projects. They have had a continuous string of projects that have affected the resources on staff. As workload has exceeded capacity they have managed to add sufficient resources to maintain an effective balance. They have built a strong legacy of extreme reliability over the years and find the user community having some difficulty accepting the lack of "first time –every time" reliability that seems to be difficult to achieve in a wireless environment. They continue to pursue improved service; however it is challenging to determine specific factors that can cause an excellent signal to be only a meter away from a marginal one.

Lifecycle

All the wireless hardware in the district is currently in a five to seven year replacement cycle.

Conclusion

Each district has its own objectives, budget and time line. Wireless networks have their own set of challenges and limitations that both need to be addressed and communicated to the user community. Wolf Creek has created clear guidelines relating to the level support as it relates to personally-owned devices and devote their time to ensuring the network infrastructure is operating properly.

Grande Prairie Public School District (GPPSD)

Grande Prairie Public School District's wireless network is the only Cisco system among the school authorities interviewed. The wireless deployment for coverage is complete and now is undergoing technology upgrades as it continues to improve capacity. The system was deployed in phases that matched the funding available for the implementation.

Cost Saving Techniques

Grande Prairie Public used a variety of funding mechanisms to provide the infrastructure required for its wireless network. The first phase was primarily consultant driven with the funds coming from an Air of Excellence Grant for its implementation. Phase 2 was in large part funded from a general technology grant. Phase 3 was funded from capital budgets used for the wireless deployments in new schools. The district also purchased an extra 10% of APs to provide for a more seamless response to capacity requirements.

Vendor Selection

Grande Prairie Public selected Cisco as its wireless solution vendor, which has allowed for a complete Cisco solution from APs to switching and routing technology. The Cisco Wireless Control System (WCS) is the wireless management platform.

Grande Prairie Public Summary

- *6,000 Students*
- *700 Staff*
- *14 Schools*
- *14 Complete Wireless Networks*
- *Cisco Solution. Wireless Controllers and Thin Access Points*
- *8 IT staff*

Implementation

The initial rollout of wireless in schools was primarily handled by consultants, who worked with in-house resources where possible to save costs. Consultants assisted with network design, including performing site surveys, recommending wireless AP and controller hardware and performing initial setup of Cisco WCS management system. The IT staff used this as a training opportunity, allowing the district to bring installations in-house as the system matured. A large part of the infrastructure is still 10/100. So as well as implementing "n" AP technology, a plan is in place to migrate the switching technology to Gigabit to support the AP capacity as well has the infrastructure backhaul required. The main driver for this is wireless "n" readiness. The goal is to have 100% of Gigabit backhaul deployed by the summer of 2012.

Security

Grande Prairie Public's entire wireless system and routing technology is Cisco, and the firewall is provided by a Microsoft ISA server. With the distributed nature of a more rural network, distributed Internet access will also alleviate some of the traffic bottlenecks that are being experienced. There is still some planning required for the system to determine the extent of distributed versus centralized firewall model to be employed. Grande Prairie Public continues to investigate load balancing technology as well as requirements for the business critical services to ensure the solution selected will provide them the security, capacity and flexibility the system requires. The system allows for 24 hour access to the network, and domain traffic is filtered separately from the Guest network. The Guest network traffic, which uses web authentication, is routed to the Internet via a separate firewall and Internet connection.

Maintenance and Support

A wireless network requires additional support resources. Combining new types of system complaints and problems compared to a wired network, there is also the learning curve for IT staff to become confident in their skills in troubleshooting and managing an increased workload. Now that the system has matured, the troubleshooting is minimal, and the majority of additional wireless work arises from adding capacity from the original coverage model. Some of the physical cabling required is handled by contract installation.

Lifecycle

With the wireless network deployment having begun when the abg AP was the most common AP, there will be the need to retire some of the legacy APs. Some of the original APs will have to be replaced within a year or two and as with most of the school districts, the change is mostly related to capacity and new technology as opposed to equipment failure. Grande Prairie Public has a five-year, lease-based replacement plan for servers and four years for workstations. All wireless hardware was purchased with initial funding. Aside from replacing abg APs with n-compliant models, the district is not planning to refresh this hardware for the next three years. As the next wireless standard is developed to replace 802.11n, the district will continue to assess the need to upgrade.

Conclusion

Grande Prairie Public continues to complement its complete wireless coverage model with advancements in capacity, infrastructure and acquiring the skill sets to respond to the wireless system deployment needs. As most school authorities have seen, the maintenance of a wireless network is somewhat more nebulous than a wired only network, however their planning and response has been a good example for all.

Appendix B Implementation Resources

The implementation phase should not be daunting or filled with surprises. As addressed in Chapter 3, the entire project plan needs to be taken into consideration.

Checklist

Below is a sample, high level checklist to assist with WLAN implementation. It includes items that are required before WLAN implementation, such as infrastructure upgrades. WLAN vendors will have specific project plans and checklists that include proprietary or unique steps in setting up their hardware and software.

Note that the pre-WLAN projects could likely take more resources and time than the actual WLAN portion of the setup. Each below listed item could be expanded to include subsequent projects and new school sites.

Sample WLAN Project Plan

Step	Plan and Communicate	# of Days	Running Total Time in Days
1.00	Determine the scope including the number of schools, size of the required coverage area(s), number of users to be supported	2	2
1.01	Set goals and expectations	0	2
1.02	Define roles of project team members	1	3
1.03	Define budget	1	4
1.04	Draft mid- to long-term plans (1 to 5 years) to allow for scalability in line with strategic business planning	1	5
1.05	Decide on wireless encryption and authentication protocol	1	6
1.06	Determine minimum security requirements	1	7
1.07	Identify compatibility and/or required upgrades and configuration changes to existing hardware, software, network architecture and maintenance/support structure (e.g. Authentication server, Internet connectivity, backbone switching architecture, NICs, VLAN supporting firewalls, etc.)	4	11
1.08	Outline usage and applications to be run on the WLAN to estimate additional bandwidth, speed and latency requirements	2	13
1.09	Select target client:AP ratio, approximate cost per AP and percentage of AP to total budget (e.g. 10:1, $250 and 20%)	0	13
1.10	Determine user policies for the wireless network	1	14
	Sub-Total	14	14
	Site Survey		
2.00	Obtain floor plans for all implementation sites	3	17
2.01	Determine how many APs it will take to provide a signal to the desired coverage area	1	18
2.02	Physical AP placement map	1	19
2.03	Identify signal trouble areas and physical construction or environmental challenges	0	19
2.04	Diagram channel layout of APs	1	20
2.05	Confirm hardware compatibility (include desired legacy hardware, new hardware and current or future for student owned device standards)	2	22
2.06	Verify that each APs location is physically secure	0	22
2.07	Verify that there is a power source near the intended location for each AP or PoE compatibility	1	23
2.08	Confirm there is a way to run a patch cable between your wired network and each AP and/or APs to be used as repeaters.	1	24

2.09	List specialized antennae requirements	0	24
2.10	Determine AP network cabling distances and are within CAT-5 or 6 limits (~100m)	1	25
	Sub-Total	11	25
	Procure Hardware, Software, Services and Training		
3.00	Research and review vendor WLAN solutions	3	28
3.01	Meet top two to three WLAN vendors for face-to-face presentations on their solutions	5	33
3.02	Purchase infrastructure upgrades identified in planning stage (e.g. District head office and/or school site WAN speed increase from 10Mb/s to 60Mb/s and switch upgrades from 100Mb/s to 1Gbps)	21	54
3.03	Buy the necessary AP, controllers, management software, and wireless NICs	5	59
3.04	Record the MAC address of all hardware	1	
3.05	Purchase other upgrades identified in planning stage	5	64
3.06	Record and distribute all vendor and out-sourced service company or VAR technical support contact information to implementation team	1	65
3.07	Register with all vendors using a centralized and common email address for alerts, support notifications, etc. (e.g. WLAN@yourdomain.com which is aliased to all relevant members)	1	66
	Sub-Total	42	66
	WLAN Implementation and Security		
4.00	Configure and install WLAN controller	1	67
4.01	Install a pilot set of APs at one location	1	68
4.02	Configure clients	1	69
4.03	Test and fine tune client:AP ratio	1	70
4.04	Adjust AP and antennae placement	1	71
4.05	Roll-out all APs at all locations	3	74
4.06	Record physical location of all hardware (by MAC addresses), use floor plans	1	75
4.07	Configure remaining clients	1	76
4.08	Test and fine tune	3	79
4.09	Configure and implement security settings for VPN, VLAN, NAC and/or other hardware and software (advised to perform on pilot area, test, then roll-out)	5	84
4.10	Vendor product training on Controller management software. Reset all passwords to high level of entropy, get familiar with interface, features, capabilities and reports	3	87
	Sub-Total	21	87
	Assess project and repeat above steps as necessary	**10**	**97**
	Integrate WLAN into IT strategy and maintenance and support structure	**10**	**107**

Information Sharing

All technical implementation team members should have a master project folder that includes the following items:

- Alberta Education WLAN Best Practices Guide;
- District Security Policy;
- Vendor contact;
- Project team contact;
- IT management contact;
- Other contact info (school or district maintenance, etc.);
- Project plan;
- Floor plan of all sites;

- Roles, goals and responsibility list;
- Schedule;
- Deadlines;
- All associated vendor documentation (hardware, software or other); and
- Blank inventory sheets. Do not underestimate pen and paper here.

Time and frustration are the two biggest items saved by having clear and consistent communication amongst the technical implementation team right up to the senior management ultimately responsible for the project.

Roll-Out of Wireless Networks

Regardless of the size of the school district and the depth of its IT staff, the implementation team should follow the pilot methodology. This will save time in the overall project, and offer an opportunity for junior IT staff to gain valuable experience and training alongside senior members of the technical implementation team. The pilot phase should not be rushed as it provides a valuable knowledge transfer to the junior IT staff members, which is essential to build in-house skill-set.

Technical hurdles must be overcome during the pilot phase to minimize any potential negative impact on wireless use in schools.

Documentation

Inventory of Wireless Devices

All serial numbers, makes, models, MAC addresses and locations should be documented. This information will be required when contacting vendor support.

Read all Vendor Information

Valuable tips and information will be recorded in the vendor documentation. Generally, the vendor wants the setup experience to be positive, and will pack as much helpful data into the documents as possible.

Record All Support and Contact Information

Record all technical support numbers and support contract details. This information should be delivered to any technician on the implementation team who will be performing setup or trouble-shooting. Having this information will greatly speed up implementation.

Include internal IT project team members and senior management for clear and immediate communication as required during a swift setup.

Trouble Shooting Tips

Challenges can arise when implementing a WLAN. The following checklist should help school authorities' technical teams resolve many of these challenges.

When a wireless network fails, there are eight areas to look to first:

1. Swap the troubled AP for hardware troubleshooting;
2. Test signal strength;
3. Try changing channels;
4. Verify the SSID;

5. Verify client encryption settings;
6. Verify AP connectivity ;
7. Verify wireless controller connectivity; and
8. Verify connectivity to DHCP server.

WLAN Performance Testing and Tuning

Testing Methods and Devices

Wireless LAN assurance tools are available from various vendors as either hardware or software, including free versions to be placed on a laptop. This will help with the initial site survey and ongoing management for items like interference, signal analysis and rogue AP detection. Here are a few vendors listed to begin your research in this area:

Fluke Networks:	www.flukenetworks.com/wirelss
Air Magnet:	www.airmagnet.com/products/laptop.htm
WildPackets:	www.wildpackets.com/products/omni/overview/omnipeek_analyzers
AirMagnet:	www.airmagnet.com
Network Stumbler	www.netstumbler.com This is free software to be loaded onto a Wi-Fi enabled PC
Tektronix	http://www.tek.com/products/communications/products/wireless/index.html
Cisco	Spectrum Expert www.cisco.com

There are also devices called spectrum analyzers that identify arbitrary wireless signals. They are typically too expensive ($10,000+) to purchase outside of large enterprises or service providers and require specific training for proper use.

Fine Tuning

Measuring Signal Strength

In conducting the site survey, make sure that the proper equipment and tools are available and present. That equipment can be relatively simple, including the APs, antennae and wireless stations that will actually be used in the deployment. Place the AP in locations where it is likely to achieve appropriate coverage and then measure the result. With the AP in a given spot, move the wireless station to various locations and measure the signal strength, noise level, packet retry count, signal to noise ration and other data rates produced. Take several measurements from each location to assure consistent results.

Appendix C Glossary of Terms and Acronym Key

AES	Advanced Encryption Standard
AP	Access Point. A generic description given to a network access device. It may be a wireless router.
BSS	Basic Service Set. Describes a wireless network with a permanent installation where one of the devices (an AP) forwards the frames between stations as well as between the stations and a wired network.
BSSID	Basic Service Set Identifier. Not to be confused with SSID. In an infrastructure network or BSS, this is the MAC address of the AP. In an IBSS, this will be a random number in the form of a MAC address. However, due to the ability of the clients to join and leave the IBSS, this ID can stay with the network as long as it is operational.
CA	Collision Avoidance
CSMA	Carrier Sense Multiple Access
DSSS	Direct Sequence Spread Spectrum. A technology that uses more bandwidth than is actually required to transmit the signal. It achieves this by taking the information "bits" and representing each bit with a predetermined string of 1's and 0's. While this may seem like a waste, it creates a signal that is resilient to interference and allows it to be transmitted at very low power values.
ESS	Extended Service Set. Describes a wireless with multiple APs sharing a common SSID. This allows clients to roam between APs while maintaining a network connection.
FHSS	Frequency Hopping Spread Spectrum. A technology that uses frequency agility to spread data over a wide portion of the spectrum. The main items are how long the radios stay on a channel, how many channels are in its hop pattern and how fast it can hop to another channel.
HT-Greenfield	This refers to a network of only 802.11n devices, all 802.11a/b/g devices have been prevented from network access
IBSS	Independent Basic Service Set. Describes a wireless network that is made up on client devices only. It allows short-term ad-hoc connections and it often referred to as an ad-hoc or peer-peer network.
IDP	Intrusion Detection and Prevention
IDS	Intrusion Detection System
IEEE	Institute Of Electronic And Electrical Engineers
IP-PBX	IP-Private Branch Exchange
IPS	Intrusion Prevention System
MCS	Modulation and Coding Scheme refers to the variety of data rates that are possible with 802.11n. MCS 0 to 15, with two possible guard band timers and two possible spectrum bandwidths
MIMO	Multiple Input, Multiple Output each stream in 802.11n has a maximum data rate of 150Mb/s. Current radio technology uses two streams for a maximum aggregate data rate of 300 Mb/s.
MSP	Mobile Services Platform
NAC	Network Admission Control. Describes is a set of technologies and solutions designed specifically to help ensure that all wired and wireless endpoint devices (such as PCs, laptops, servers, and PDAs) accessing network resources are adequately protected from security threats.
OFDM	Orthogonal Frequency Division Multiplexing. OFDM is a technology that is *spread spectrum like*, although it is not a true spread spectrum technology. It takes information and multiplexes it onto a group of carefully planned out sub-carriers. Each sub-carrier has a relatively low data rate, but by transmitting data in parallel on these sub-carriers, it creates the highest throughput of any current technology.
QOS	Quality Of Service
RF	Radio Frequency

SMB	Small And Midsize Business
SOHO	Small Office/Home Office
SSID	Service Set Identifier. Describes a particular network, comprisng of 2 - 32 unique case sensitive ASCII characters.
VoIP	Voice Over IP
VoWLAN	Voice Over WLAN
VPN	Virtual Private Network
WCS	Wireless Control System
WEP	Wired Equivalent Privacy. The initial layer 2 method of encrypting data over a wireless link. It requires the entry of a static key on all network devices.
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access. This is a certification released by theWi-Fi alliance to provide improved security during the time that 802.11i was being developed. It defines advanced modes of authentication and encryption as well as being backwards compatible with WEP.
WPA2	Wi-Fi Protected Access 2 is the certification released by the Wi-Fi Alliance which is based on the completed 802.11i standard.

Appendix D Vendors

Some Vendors of WLAN Solutions Include:

Vendor	Website Address
Aerohive	www.aerohive.com/
Alcatel-Lucent	www.alcatel-lucent.com
Aruba Networks	www.arubanetworks.com
Bluesocket	www.bluesocket.com
Brocade	www.brocade.com
Cisco Systems	www.cisco.com
Enterasys Networks	www.enterasys.com
Extricom	www.extricom.com
Extreme Networks	www.extremenetworks.com
Hewlett-Packard	www.hp.com
Meru Networks	www.merunetworks.com
Ruckus Wireless	www.ruckuswireless.com
Siemens	www.siemens.com
Motorola	www.motorola.com
Trapeze Networks	www.trapezenetworks.com
Xirrus	www.xirrus.com

Note: The scope of this Guide does not allow for a thorough review and inclusion of product information from all vendors. The above websites are listed to allow school authorities to research additional vendor information.